

Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Материалы
XXIV Международной научно-технической конференции
(Республика Беларусь, Минск, 8 апреля 2026 года)

Редакционная коллегия:

О. В. Бойправ, Т. В. Борботько, Г. В. Давыдов,
Л. М. Лыньков, Л. А. Шичко

НАУЧНЫЙ ПРОГРАММНЫЙ КОМИТЕТ:

В. А. Богуш	ректор БГУИР, председатель (Республика Беларусь);
О. В. Бойправ	зав. кафедрой защиты информации БГУИР, зам. председателя (Республика Беларусь);
В. Р. Стемпицкий	проректор по научной работе БГУИР (Республика Беларусь);
Е. Е. Бегимбаева	зав. кафедрой кибербезопасности Алматинского университета энергетики и связи им. Г. Даукеева (Республика Казахстан);
Т. В. Борботько	директор Государственного предприятия «НИИ ТЗИ» (Республика Беларусь);
М. Г. Гасанов	зав. кафедрой радиотехники и телекоммуникаций Азербайджанского технического университета (Азербайджанская Республика);
А. В. Иванов	зав. кафедрой защиты информации Новосибирского государственного технического университета (Российская Федерация);
В. А. Касумов	декан факультета информационных и компьютерных технологий Бакинского инженерного университета (Азербайджанская Республика);
И. Х. Норматов	проф. кафедры информационной безопасности Национального университета Узбекистана (Республика Узбекистан);
Р. Ж. Сатыбалдиева	зав. кафедрой кибербезопасности, обработки и хранения информации Казахского национального исследовательского технического университета имени К. И. Сатпаева (Республика Казахстан);
Ю. С. Харин	директор НИИ прикладных проблем математики и информатики Белорусского государственного университета (Республика Беларусь);
А. Г. Филиппович	начальник управления Оперативно-аналитического центра при Президенте Республики Беларусь (Республика Беларусь);
А. В. Хижняк	ведущий научный сотрудник научно-исследовательской лаборатории факультета связи и автоматизированных систем управления войсками Военной академии Республики Беларусь (Республика Беларусь);
А. А. Хорев	зав. кафедрой информационной безопасности Национального исследовательского университета «МИЭТ» (Российская Федерация);
А. А. Шелупанов	президент Томского государственного университета систем управления и радиоэлектроники (Российская Федерация)

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ:

О. В. Бойправ	зав. кафедрой защиты информации БГУИР, председатель;
Е. С. Белоусова	доц. кафедры защиты информации БГУИР, зам. председателя;
В. С. Мокеров	стажер младшего научного сотрудника научно-исследовательской лаборатории 5.3 научно-исследовательской части БГУИР;
Е. В. Бакунова	нач. ОМНК НИЧ БГУИР

Т38 **Технические средства защиты информации : материалы XXIV Междунар. науч.-техн. конф. (Респ. Беларусь, Минск, 8 апр. 2026 г.) / редкол.: О. В. Бойправ [и др.]. – Минск : БГУИР, 2026. – 436 с.**
ISBN 978-985-543-880-0.

Издание содержит тезисы докладов, тематика которых посвящена вопросам технической и криптографической защиты информации, элементной базе средств защиты информации, нормативно-правовому регулированию и подготовке специалистов в области защиты информации.

УДК 004.056.5
ББК 32.972.5

ISBN 978-985-543-880-0

© УО «Белорусский государственный университет информатики и радиоэлектроники», 2026

ОГЛАВЛЕНИЕ

СТАТЬИ ПО МАТЕРИАЛАМ ПЛЕНАРНЫХ ДОКЛАДОВ

Gasimov V.A., Zahidova G.A., Valiyeva A.A., Zeynalli-Huseynzada L.R. Security issues in IoT devices.....	13
Gasimov V.A., Zahidova G.A., Zeynalli-Huseynzada L.R. Prospects of using lightweight cryptography in IoT devices.....	18
Норматов И.Х., Дадажанов Р.Н., Атаджанов М.Н. Алгоритмическое моделирование информационной безопасности на основе таблиц функционирования.....	23
Макаров А.М., Писаренко Е.А., Гаджимурадов Б.М. Обобщенная модель иерархической информационной системы с распределенным реестром в цифровой среде управления государством.....	33

СТАТЬИ ПО МАТЕРИАЛАМ СЕКЦИОННЫХ ДОКЛАДОВ

Зайкова С.А. Безопасность данных в спортивных приложениях.....	37
Воробьев С.Ю., Ханчевский Е.А. Реализация требований СТБ ISO/IEC 27001-2024 в деятельности предприятия энергетической отрасли.....	40
Клиндухов Я.А., Мажаева С.Д., Бойправ О.В. Применение обучающих игр для формирования специальных навыков по защите от угроз информационной безопасности.....	44
Воронина А.М. Формирование компетенций в области защиты информации при подготовке кадров для цифровой экономики Республики Беларусь.....	49
Мищенко В.Н. Моделирование выходных характеристик полевых транзисторов с использованием графена и его модификаций в диапазонах СВЧ и КВЧ.....	52
Ручаевская Е.Г., Шаталова В.В. Аспекты обеспечения безопасности информационных систем.....	56
Савельева М.Г. Программное средство для осуществления стеганографического преобразования на основе модификации полутоновых оттенков растрингованных документов.....	58
Коваленко Д.А., Аль-Махдави М.С.Х., Врублевский И.А. Нелинейные свойства частотной зависимости емкости структур на основе полупроводниковых графитоподобных пленок углерода.....	62
Гусаков П.Б., Макаренко К.Е. Современная методология построения средств и систем защиты информации.....	65
Одинец Д.Н. Методика анализа трафика и верификации шифрования в сотовой сети 4/5G на основе имитатора базовой станции ЮНИТЕСС.....	69
Чиж В.В. Метод предотвращения угроз в закрытой сетевой инфраструктуре на основе внутренней сегментации.....	73
Ярмольчик А.А., Гусаков П.Б. Построение доверенной среды исполнения на белорусских предприятиях.....	76
Бурко Л.А., Иванюк А.А. Метод повышения уникальности аппаратных идентификаторов плис на основе физически неклонируемых функций типа конфигурируемого кольцевого осциллятора.....	79
Серкевич Д.С., Герман Ю.О. Стеганографический метод защиты информации.....	83
Маугин И.В. Алгоритм встраивания цифрового водяного знака, устойчивый к геометрическим атакам и зашумлению.....	87
Мартинкевич Д.М., Яниславский К.О., Белоусова Е.С. Функции фильтрации и шифрования DNS-сообщений на межсетевом экране CHUWALL.....	90

Тимофеев А.М., Шляхтун Д.В., Чэнтинъюй Ли, Цзыхань Хуан. Обезличивание персональных данных на основе метода изменения состава	93
Гладинов А.Д. Многослойные тонкопленочные экраны электромагнитного излучения с развитым периодическим рельефом поверхности	97
Крамаренко А.К., Лопато А.В. Аппаратно-программные механизмы блокировки вредоносного кода	102
Sudani Н.Н. Enhancing cybersecurity resilience through an integrated artificial intelligence framework	105
Бердник А.И. Адаптация образовательных программ по информационной безопасности под требования стека отечественных ОС (на примере Astra Linux).....	109
Маевский П.К. Архитектура технической защиты и выбор доверенной элементной базы для измерительных IoT-систем.....	112
Бокун А.Г. Применение ансамблевых методов машинного обучения для фильтрации ложных срабатываний в SIEM-системах.....	115
Буневич А.А. Система подтверждения транзакций в блоках публичных блокчейн-сетей.....	120
Wang J. Development of mathematical tools for image restoration with distorted data.....	124
Алефиренко В.М., Зубрицкий Е.Д., Морозова А.Н. Анализ параметров приборов обнаружения скрытых проводов технических средств несанкционированного съема информации с помощью комплексного геометрического показателя качества	126
Сидоренко А.В., Сергеев И.В. Алгоритм постквантового шифрования с использованием хаотических отображений и принципа кубика рубика.....	129
Мельникова Т.А., Васькевич В.В. Сравнительный анализ существующих методов обнаружения brute-force атак в системах аутентификации	134
Кайкы М.Н., Иванюк А.А. RS-защелка как источник случайности в режиме инициализации.....	138
Nguyen М.Н., German Yu.O. Extracting data from the hash memory using an error key	141
Крамаренко А.К., Егоренков Н.Д. Аппаратные функции безопасности в формировании рыночной стоимости IT-платформ	143
Герасимов А.С., Макаренко К.Е. Методы защиты алгоритма BelT от атак с внедрением ошибок.....	147
Шмавгонец А.В. Анализ уязвимостей и угроз в корпоративных сетях	150
Баженова И.В. Анализ характеристик твердотельных устройств в СВЧ диапазоне.....	154
Баженова И.В. Генераторы СВЧ с внешней дополнительной обратной связью	157
Шерышев Р.В., Коваленко Д.А., Ободо Ч.В. Прогнозирование поведения объекта с использованием систем интеллектуального видеонаблюдения.....	159
Боровиков С.М. Сравнение по критериям Байеса и Неймана-Пирсона моделей прогнозирования надежности изделий электронной техники	163
Боровиков С.М., Гришечкин Е.Д., Будник А.В. Оценка надежности импульсных трансформаторов с учетом их конструктивных особенностей.....	166
Осипов Р.Д., Савицкий А.Ю., Игнатенко А.А. Примеры защиты от SQL-инъекций в WordPress	170
Солонович М.А., Игнатенко А.А. Постквантовые криптографические алгоритмы и применение искусственного интеллекта для повышения стойкости шифров.....	174
Славинский Г.А., Быстрова В.А., Боброва Н.Л. Применение технологий искусственного интеллекта в SIEM для минимизации ограничений правил корреляции.....	177

Wu Y., Prischepa S.L. Electrodynamic analysis of nanocomposite microwave screening via equivalent RLC circuit models.....	181
Силивонец А.С., Данилюк А.Л. Конверсия спинового тока в зарядовый в магнитном полуметалле вейля.....	185
Юнчиц Е.И., Гусаков П.Б. Архитектура модуля ИИ-агента для SIEM-систем нового поколения.....	188
Пилипенко А.О., Супрун Ф.Н. Применение ИИ-агентов в доверенной элементной базе для предиктивного обнаружения аппаратных атак	191
Качинский М.В., Станкевич А.В., Шемаров А.И. Реализация на FPGA алгоритма шифрования СТБ 34.101.31	195
Качинский М.В., Станкевич А.В., Шемаров А.И. Распараллеливание алгоритма блочного шифрования данных со сцеплением блоков.....	199
Биюмен Е.А., Маршалова К.Ц. Архитектура платформы автоматизации аудита информационной безопасности	202
Третьяков И.А., Рушечников Я.И., Данилов В.В. Алгоритм анализа количественных спектральных составляющих мощности сигнала ПЭМИН.....	206
Al-Absi Saleh S.A.E. Face recognition in low light conditions	210
Qiao X., Kedo E.S. Detection of XSS attacks and SQL injections using convolutional neural networks	212
Петров С.Н., Ермоленко Д.В., Рожкова А.С. Telegram-бот для обучения подростков основам кибербезопасности	215
Смотрук Г.С., Пулко Т.А. Организация централизованного сбора событий информационной безопасности в SIEM-системах с учетом нормативных требований	219
Петров С.Н., Пакуль Е.С., Корчинский А.А. Автоматизированный статический анализ уязвимостей мессенджера Peregrine с использованием больших языковых моделей	222
Фирсов А.А., Герасимов А.С. Автоматизированная система защищенной обработки служебной информации для органов пограничной службы	226
Лепесий И.А., Романович Е.С. Метод защиты криптографических ключей на основе генерации ложных секретов с использованием машинного обучения	230
Duong N.A., Dao T.H. Detecting cyber-attacks based on network steganography	232
Скапцов С.С., Кисель М.А. Применение схем полностью гомоморфного шифрования для обеспечения безопасности облачных вычислений.....	237
Li C. Enhancing personal data de-identification using DES-based transformation techniques.....	240
Ефремова А.Ю., Алефиренко В.М. Сравнительный анализ источников излучения для шифрования с помощью квантовых точек.....	242
Ефремова А.Ю. Сравнение технических средств спектрального анализа, используемых в квантовой криптографии	246
Герасимов В.А. Сравнительный анализ безопасности подходов к аутентификации пользователя в системах электронной цифровой подписи на основе виртуальной инфраструктуры	249
Ходжамаммедов М.М. Применение постквантовой криптографии для защиты информации в цифровых системах	253
Ходжамаммедов М.М., Джумагылджов Ю.Т., Мухаммедов М.М. Техническая защита информации в условиях цифровой трансформации и роста киберугроз.....	256
Савчук В.В. Квантовое распределение ключей как перспективный метод криптографической защиты информации	259
Ручаевская Е.Г., Буйневич Е.Д. Основные меры по снижению рисков SQL-инъекций.....	262

Давыдов Г.В., Давыдов И.Г., Потапович А.В., Попов В.А. Стенды для моделирования воздействия удара на радиоэлектронные компоненты.....	266
Барковская К.Н., Мадвейко С.И. Применение плазмохимического травления в обратном инжиниринге для анализа аппаратных средств защиты информации	269
Юров М.Д., Чижик В.В. Нормативно-правовое регулирование в сфере информационной безопасности в Республике Беларусь	273
Денскевич А.Д. Сравнительный анализ отечественных и зарубежных стандартов оценки разборчивости речи для защиты информации.....	277
Коржова И.А. Сравнение рекуррентных нейронных сетей для обработки речевых сигналов.....	280
Тимофеев А.М., Шляхтун Д.В. Уменьшение объема хранимых персональных данных при их обезличивании на основе метода изменения состава	286
Юров М.Д., Чижик В.В. Кадровый потенциал информационной безопасности в Республике Беларусь	290
Богушевич О.А., Гайко А.С. Утечка персональных данных: методика оценки критичности инцидента.....	294
Асиненко А.М. Средства электромагнитного подавления беспилотных летательных аппаратов	297
Приходченко Н.А. Внедрение межсетевого экрана уровня приложений на предприятии	300
Гавришев А.А. Совершенствование отдельных нормативных аспектов деятельности управленческих кадров по информационной безопасности	304
Шустик А.О., Савицкий А.Ю. Искусственный иммунитет цифровой среды.....	307
Янович К.Д., Васькевич В.В. Адаптивное обучение специалистов по кибербезопасности: использование искусственного интеллекта и СТФ-платформ.....	311
Таран Д.С., Федоренко В.А. Постквантовая криптография: почему нам пора менять методы защиты.....	315
Маршалова К.Ц., Биюмен Е.А. Образовательный хаб для подготовки специалистов в области защиты информации	318
Руденок Д.А., Змачинская У.А. Классификация типа схемы в протоколах двусторонних вычислений на основе анализа транскрипта.....	321
Муравицкий Д.Г., Федоренко В.А. Защита информации при проведении специальной военной операции.....	325
Мальцев В.Л., Возмитель В.В., Матяс Е.В. Влияние архитектуры нейронных сетей на эффективность обнаружения признаков шифрования	328
Мальцев В.Л., Олексин С.А., Самосюк А.И. Обеспечение целостности документооборота через гибридный блокчейн и изолированное исполнение кода.....	332
Ворожцов А.О. Методика определения подлинности RFID-меток.....	335
Мойсюк-Дранько Я.А., Дубовик И.А. Защищенная система радиоуправления беспилотным летательным аппаратом с псевдослучайной перестройкой рабочей частоты и криптографическим шифрованием.....	338
Войткус И.А., Белоусова Е.С. Инструмент для OSINT-разведки и реализации техники MITRE ATT&CK T1593	342
Русак И.В. Обучающий эксперимент как основа получения моделей прогнозирования надежности полупроводниковых приборов.....	345
Пухир Г.А., Шерышев Р.В. Международный опыт государственного регулирования деятельности в сфере защиты информации.....	348

Петров Д.О., Буслюк В.В., Латий О.О., Емельянов В.А. Исследование термокомпенсации шумовых диодов для использования в устройствах промышленного интернета вещей	352
Ковальчук Н.Г., Дронина Е.А., Томашевич Л.П., Петров А.В., Каланда Н.А., Лазарук С.К. Антиотражающие покрытия на основе углеродных нанотрубок для фоточувствительных устройств	358
Галузо В.Е., Пинаев А.И. Противодымная защита многоэтажных зданий	361
Галузо В.Е., Пинаев А.И. Противодымная защита паркинга	364
Грицкевич Г.И., Пашкевич В.Э., Смолкин Ю.А., Жук Р.С., Лешко А.С., Ловшенко И.Ю. Разработка конфигурации системы освещения автоматических зондовых установок	367
Уласевич Н.И., Савельева М.Г. Адаптация стеганографического метода, основанного на изменении пространственной области, для векторных изображений формата SVG	371
Сухоцкий В.В. Актуальные достижения контроля целостности в области криптографической защиты информации	375
Митюхин А.И. Кодирование адресных последовательностей нелинейным кодом	378
Винокуров М.А., Шумило Д.А. Многоэтапная компрометация информационных систем: взлом Веб-API и генеративная обфускация полезной нагрузки	382
Назаренко Е.С., Данилюк А.Л. Влияние подложки на корреляционные функции осей случайной анизотропии в массивах наночастиц Co/CoO	385
Неслуховский Д.И., Горин Д.С. Технология автоматизированного формирования базы легитимных TLS-отпечатков	388
Хаджинова Н.В. Активная защита исполняемого кода с использованием аппаратных криптосредств и полиморфных классов C++	393
Хаджинова Н.В. Использование механизмов активной защиты в распределенных мультиагентных системах управления	397
Кушнир В.Н., Прищепа С.Л. Критерии смягчения фононного спектра монокристаллической пленки с двумерным покрытием	400
Боровой М.А., Ободо Ч.В. Анализ возможностей цифровой системы ip-видеонаблюдения для обеспечения безопасности объекта наблюдения	405
Лазарук С.К., Ореховская Т.И., Дудич В.В., Долбик А.В., Томашевич Л.П., Ефименко С.А. Алюмооксидные корпуса для защиты микросхем от внешних воздействий	408
Дудич В.В., Купреева О.В., Ореховская Т.И., Долбик А.В. Регулярные металлические матрицы для управления отражением электромагнитных волн за счет эффекта поверхностного плазмонного резонанса	411
Шаталова В.В. Особенности практико-ориентированной подготовки специалистов по информационной безопасности со средним специальным образованием	414
Абросимов М.Б., Жаркова А.В., Лобов А.А., Моденова О.В., Саяпина А.А., Калашникова З.А., Трунилина Е.А., Шабаркова А.О. О XXIV международной олимпиаде по криптографии SarCrypt	418
Шарейко М.В., Данилюк А.Л. Распределения намагниченности в нанопроводах никеля	421
Zihan Huang. Technical means of information protection	424
Золотов В.В. Формирование профессиональных компетенций специалистов по защите информации	428
Лебедев А.А. Средство программной защиты от HID-атак BadUSB	431

TABLE OF CONTENTS

ARTICLES BASED ON THE MATERIALS OF THE PLENARY REPORTS

Gasimov V.A., Zahidova G.A., Valiyeva A.A., Zeynalli-Huseynzada L.R. Security issues in IoT devices.....	13
Gasimov V.A., Zahidova G.A., Zeynalli-Huseynzada L.R. Prospects of using lightweight cryptography in IoT devices.....	18
Normatov I.Kh., Dadazhanov R.N., Atadzhanov M.N. Algorithmic model of information security based on functioning tables	24
Makarov A.M., Pisarenko E.A., Gadzhimuradov B.M. Generalized model of a hierarchical information system with distributed ledger for digital government management.....	33

ARTICLES BASED ON THE MATERIALS OF SECTIONAL REPORTS

Zaikova S. Data security in sports apps.....	37
Vorobyov S.Yu., Khanchevsky E.A. Implementation of STB ISO/IEC 27001-2024 requirements in the activities of an energy industry enterprise.....	40
Klindukhov Y.A., Mazhaeva S.D., Boiprav O.V. Application of educational games for the formation of special skills in protection against information security threats	44
Voronina A.M. Formation of information protection competencies in the training of personnel for the digital economy of the Republic of Belarus.....	49
Mishchanka V.N. Modeling of output characteristics of field-effect transistors using graphene and its modifications in the microwave and mwr range	52
Ruchaevskaya E.G., Shatalova V.V. Aspects of information systems security ensuring	56
Saveleva M.G. A software tool for performing steganographic transformation based on modification of halftone shades of rasterized documents.....	59
Kavalenka D.A., Al-Mahdawi M.S.H., Vrublevsky I.A. Nonlinear capacitance-frequency characteristics of structures with semiconducting graphite-like carbon films.....	62
Gusakov P.B., Makaranka K.E. Modern methodology for building information protection means and systems	65
Adzinets D.N. Method of traffic analysis and encryption verification in a 4/5G cellular network based on the UNITESS simulator of base station	70
Chizh V.V. Method for preventing threats in a closed network infrastructure based on internal segmentation.....	73
Yarmolchik A.A., Gusakov P.B. Building a trusted execution environment at belarusian enterprises.....	76
Burko L.A., Ivaniuk A.A. Method for increasing the uniqueness of FPGA hardware identifiers based on physically unclonable functions of configurable ring oscillators.....	80
Serkevich D.S., German Yu.O. Steganographic method of information protection.....	83
Mautsin I.V. Digital watermarking algorithm robust to geometric and noise attacks	87
Martsinkevich D.M., Yanislauskis K.A., Belousova E.S. Filtering and encryption functions of DNS-messages on the chuwall firewall.....	90

Timofeev A.M., Shliakhtun D.V., Li1 Ch., Zihan H. Depersonalization of personal data based on the method of changing the composition.....	94
Gladinov A.D. Multilayer thin-film electromagnetic radiation shields with a developed periodic surface relief.....	98
Kramarenko A.K., Lopato A.V. Hardware-software mechanisms for malicious codeblocking.....	102
Sudani H.H. Enhancing cybersecurity resilience through an integrated artificial intelligence framework	105
Berdnik A.I. Adaptation of information security educational programs to the requirements of domestic os stack (on the example of astra linux)	109
Mayeuski P.K. Architecture of technical protection and selection of trusted element base for measuring IoT-systems.....	112
Bokun A.G. Application of ensemble machine learning methods for false positive filtering in SIEM.....	115
Bunevich A.A. Transaction confirmation system in blocks of public blockchain networks.....	120
Wang J. Development of mathematical tools for image restoration with distorted data.....	124
Alefirenko V.M., Zubritsky E.D., Morozova A.N. Analysis of hidden wire detector parameters using a complex geometric quality indicator.....	126
Sidorenko A.V., Sergeev I.V. Postquantum image encryption algorithm with chaotic system and rubik's cube principle	130
Melnikova T.A., Vaskevich V.V. Comparative analysis of existing methods for detecting brute-force attacks in authentication systems	134
Kaiky M.N., Ivaniuk A.A. RS-latch as a source of randomness in initialization mode.....	138
Nguyen M.H., German Yu.O. Extracting data from the hash memory using an error key	141
Kramarenko A.K., Yahorenkau M.D. Hardware security functions in determining the market value of IT platforms	144
Gerasimov A.S., Makaranka K.E. A methods of protecting the BeLT algorithm from attacks with faults	147
Shmavgonets A.V. Vulnerability and threat analysis in corporate networks.....	150
Bazhenova I.V. Analysis of the characteristics of solid-state devices in the microwave range.....	154
Bazhenova I.V. Microwave generators with external additional feedback.....	157
Sheryshev R.V., Kavalenka D.A., Obodo Ch.W. Predicting object behavior using intelligent video surveillance systems	159
Borovikov S.M. Comparison of reliability prediction models for electronic products with of Bayesian and Neyman-Pearson criteria	163
Borovikov S.M., Grieshechkin E.D., Budnik A.V. Reliability assessment of pulse transformers with consideration of their design features.....	167
Osipov R.D., Savitsky A.Yu., Ignatenko A.A. Examples of SQL injection protection in wordpress	170
Solonovich M.A., Ignatenko A.A. Post-quantum cryptographic algorithms and the application of artificial intelligence to enhance the strength of ciphers.....	174
Slavinsky G.A., Bystrova V.A., Bobrova N.L. Application of artificial intelligence technologies in SIEM to minimise the limitations of correlation rules	178
Wu Y., Prischepa S.L. Electrodynamic analysis of nanocomposite microwave screening via equivalent RLC circuit models.....	181

Silivonets A.S., Danilyuk A.L. Conversion of spin current to charge current in a magnetic Weyl semimetal	185
Yunchits E.I., Gusakov P.B. AI-agent module architecture for next-generation SIEM systems	188
Pilipenka A.O., Suprun F.N. Application of ai agents in a trusted hardware components for predictive detection of hardware attacks.....	192
Kachinsky M.V., Stankevich A.V., Shemarov A.I. FPGA implementation of the STB 34.101.31 encryption algorithm	195
Kachinsky M.V., Stankevich A.V., Shemarov A.I. Parallelization of a block cipher algorithm with cipher block chaining	199
Biyumen Y.A., Marshalava K.C. Software complex architecture for automated information security audits	203
Tretiakov I.A., Rushechnikov I.A.I., Danilov V.V. Algorithm for analyzing the quantitative spectral components of the tempest signal power.....	206
Al-Absi Saleh S.A.E. Face recognition in low light conditions	210
Qiao X., Kedo E.S. Detection of xss attacks and sql injections using convolutional neural networks	212
Petrov S.N., Ermolenko D.V., Rozhkova A.S. Telegram bot for teaching teenagers the basics of cybersecurity	216
Smatruk H.S., Pulko T.A. Implementation of centralized collection of information security events in SIEM systems subject to regulatory requirements	219
Petrov S.N., Pakul Y.S., Korchinsky A.A. Automated static vulnerability analysis of the peregrine messenger with large language models	223
Firsov A.A., Gerasimov A.S. Automated system for secure processing of official information for the border guard service	226
Lepesy I.A., Romanovich E.S. Method of protecting cryptographic keys based on generation of false secrets using machine learning.....	230
Duong Ngoc Anh, Dao Thanh Huong. Detecting cyber-attacks based on network steganography.	232
Skapcov S.S., Kisel M.A. Application of fully homomorphic encryption schemes to secure cloud computing.....	237
Li C. Enhancing personal data de-identification using des-based transformation techniques.....	240
Yafremava A.Y., Alefirenko V.M. Comparative analysis of radiation sources used for encryption based on quantum dots	243
Yafremava A.Yu. Comparison of spectral analysis instruments used in quantum cryptography.....	246
Gerasimov V.A. Comparative analysis of security of user authentication approaches in electronic digital signature systems based on virtual infrastructure	250
Hojamammedow M.M. Application of post-quantum cryptography for information security in digital systems	253
Hojamammedow M.M., Jumaglyjov Y.T, Muhammedov M.M. Technical information security in the context of digital transformation and cyber threats.....	256
Savchuk V.V. Quantum key distribution as a promising method of cryptographic information security	259
Ruchaevskaya E.G., Buinevich E.D. Key measures to reducing the risks of SQL injection	263

Davydau H.V., Davydau I.H., Patapovich A.V., Papou V.A. Stands for simulating the impact effect on radioelectronic components.....	266
Barkouskaya K.M., Madveika S.I. Application of plasma etching in reverse engineering for the analysis of hardware information security	270
Yurau M., Chizhik V. Normative legal regulation in the field of information security in the Republic of Belarus	273
Denskevich A.D. Comparative analysis of domestic and foreign standards for speech intelligibility assessment in information security.....	277
Korzhova I.A. Comparison of recurrent neural networks for speech signal processing.....	281
Timofeev A., Shliakhtun D. Reducing the volume of stored personal data by depersonalizing it based on the method of changing the composition.....	287
Yurau M., Chizhik ... V. Human resource potential in the field of information security in the Republic of Belarus	290
Bogushevich O.A., Gayko A.S. Leakage of personal data: methodology for assessing the criticality of an incident.....	295
Asinenko A.M. Means of electromagnetic suppression of unmanned aerial vehicles	297
Pryknodchenko N.A. Implementation of a Web application firewall at an enterprise.....	301
Gavrishev A.A. Improvement of certain normative aspects of management personnel on information security	304
Shustik A.O., Savitsky A.Yu. Artificial immunity of the digital environment.....	308
Yanovich K.D., Vaskevich V.V. Adaptive training of cybersecurity specialists: using AI and CTF platforms.....	312
Taran D.S., Fedorenko V.A. Post-quantum cryptography: why it's time to change protection methods	315
Marshalava K.C., Biyumen Y.A. Educational hub for training specialists in the field of information security	318
Rudenok D., Zmachynskaya U. Classification of circuit type in two-party computation protocols based on transcript analysis.....	322
Muravitski D.G., Fedorenko V.A. Information security during a special military operation	325
Maltsau V., Vozmitel V., Matyas E. Influence of neural network architecture on the efficiency of encryption feature detection.....	329
Maltsau V., Aleksin S., Samasiuk A. Providing document flow via a hybrid cable and isolated code execution	332
Voroztsov A.O. Method of defining the RFID tags identity	335
Moisiuk-Dranko Y.A., Dubovik I.A. A secure radio control system for an unmanned aerial vehicle with frequency-hopping spread spectrum and cryptographic encryption	339
Voitkus I.A., Belousova E.S. Automation of OSINT intelligence based on MITRE ATT&CK T1593 technique	342
Rusak I.V. Teaching experiment as the basis for obtaining models for predicting the reliability of semiconductor devices	345
Pukhir H.A., Sheryshev R.V. International experience in state regulation of information protection.....	349

Petrov D.O., Buslyuk V.V., Latii O.O., Emelyanov V.A. Investigation of thermal compensation of noise diodes for use in industrial internet of things devices	352
Kovalchuk N.G., Dronina E.A., Tomashevich L.P., Petrov A.V., Kalanda N.A., Lazarouk S.K. Carbon nanotube-based anti-reflective coatings for photosensitive devices	358
Galuzo V.E., Pinaev A.I. Smoke protection of multi-story buildings	361
Galuzo V.E., Pinaev A.I. Smoke protection for parking	364
Gritskevich G., Pashkevich V., Smolkin Y., Zhuk R., Leshko A., Lovshenko I. Development of a lighting system configuration for automatic probe stations	368
Ulasevich N.I., Savelieva M.G. Adaptation of a steganographic method based on spatial domain modification for SVG vector images.....	371
Sukhotski V.V. Current advances in integrity control in cryptographic information protection current advances in integrity control in cryptographic information protection	371
Mitsiukhin A. Encoding address sequences with nonlinear code	378
Vinokurov M., Shumilo D. Multistage compromise of information systems: web API hacking and generative payload obfuscation	382
Nazarenka K.S., Danilyuk A.L. Influence of the substrate on the correlation functions of random anisotropy axes in arrays of Co/CoO nanoparticles	385
Neslukhovskiy D.I., Gorin D.S. Technology for automated construction of a database of legitimate client TLS fingerprints	389
Khajynava N.V. Active protection of executable code using hardware cryptographic means and polymorphic C++ classes	393
Khajynava N.V. Using active protection mechanisms in distributed multi-agent control systems ...	397
Kushnir V.N., Prischepa S.L. Criteria for softening the phonon spectrum of a monoatomic crystalline film with 2D coating.....	401
Borovoy M.A., Obodo Ch.W. Analysis of the capabilities of a digital IP video surveillance system to ensure the security of the object under survey	405
Lazarouk S.K., Orekhovskaya T.I., Dudich V.V., Dolbik A.V., Tomashevich L.P., Efimenko S.A. Alumina packages for protecting microcircuits from external influences.....	408
Dudich V.V., Kupreeva O.V., Orekhovskaya T.I., Dolbik A.V. Regular metal matrices for controlling electromagnetic waves reflection due to the effect of surface plasmon resonance	411
Shatalova V.V. Features of practice-oriented training of information security specialists with secondary specialized education	414
Abrosimov M.B., Zharkova A.V., Lobov A.A., Modenova O.V., Sayapina A.A., Kalashnikova Z.A., Trunilina E.A., Shabarkova A.O. About the XXIV international cryptography olympiads SarCrypt ..	418
Shareiko M.V., Danilyuk A.L. Magnetization distributions in nickel nanowires.....	421
Zihan Huang. Technical means of information protection	424
Zolotov V.V. Formation of professional competencies of information security specialists	428
Lebedev A.A. Software protection against BadUSB HID-attacks	431

СТАТЬИ ПО МАТЕРИАЛАМ ПЛЕНАРНЫХ ДОКЛАДОВ ARTICLES BASED ON THE MATERIALS OF THE PLENARY REPORTS

UDC 004.056

SECURITY ISSUES IN IoT DEVICES

V.A. Gasimov, G.A. Zahidova, A.A. Valiyeva, L.R. Zeynalli-Huseynzada
Baku Engineering University, Baku, Azerbaijan

Abstract. Although the widespread use of Internet of Things (IoT) technologies increases the efficiency of information systems, the limited computing capabilities and weak security mechanisms of IoT devices make them vulnerable to various cyberattacks. This thesis analyzes the main security problems occurring in IoT devices, a real cyber incident example, and effective protection methods. As a result, it is determined that IoT security requires a complex and multi-level approach.

Keywords: IoT; cybersecurity; authentication; encryption; botnet; DDoS; firmware; network security; security risk; defense mechanism.

Introduction

The Internet of Things (IoT) is a technology that enables physical objects, sensors, and various smart devices to communicate with each other via the Internet and exchange information. The IoT system has the ability to collect, process, and transmit information in real time. This technology creates integration between the physical environment and digital systems, making management processes more efficient and automated. The application areas of IoT are quite wide. Remote monitoring of patients in the healthcare sector, automation of production processes in industry, intelligent management systems in transportation, productivity monitoring in agriculture, and smart home systems are some of the main areas where IoT is widely used. This technology not only increases economic efficiency, but also expands operational decision-making capabilities.

According to reports from international organizations such as Cisco Systems and Gartner, billions of IoT devices are in use worldwide and are increasing every year. However, the widespread use of IoT devices has also raised security concerns. Poor protection of these devices can lead to cyberattacks, data leaks, and even disruption of critical infrastructure. Therefore, investigating security issues in IoT devices is of great scientific and practical importance.

Primary Security Issues

The widespread adoption of the Internet of Things ecosystem and its application in various fields have made security issues even more critical. Unlike other information systems, IoT devices are characterized by a lack of computing power, poor memory resources, as well as energy constraints.

In addition, IoT devices are used in an open network environment, but they are not configured with the required security features. This has made IoT systems easy targets for cyber attackers.

The concerns in IoT security include both technical and organizational issues. It involves the protection of information systems in a manner that ensures the integrity, availability, and confidentiality of the information are not compromised in the hands of unauthorized persons. However, the risks are not limited to the devices alone but also the infrastructure that houses the devices.

The primary security issues associated with IoT devices are as follows.

1. *Inadequate Authentication and Authorization Mechanisms.* Perhaps one of the most common security issues when it comes to IoT devices starts right at the very beginning, as many devices are preconfigured with a default username/password combination. In many cases, the end user never bothers changing this combination. As a result, attackers have it very easy when it comes to launching a brute force attack. And then, of course, there is the role-based access control, which is not very well implemented in many cases, allowing attackers to gain access to many more rights than they should ever need. For example, someone who should only have 'read-only' rights could end up being granted the master key. And if the authentication process is not robust enough, then the threat of botnet attacks looms very large.

2. *Encryption and data protection issues.* Data security in IoT devices raises two important issues: Data in Transit, Data at Rest.

Data in Transit: In many IoT systems, data is sent over unencrypted channels, e.g., HTTP. This leaves the system open to a "Man-in-the-Middle" attack, where the hacker gains access to the network, allowing him to observe, modify, or even forge the data stream.

Data at Rest: Inadequate handling of cryptographic algorithms, improper handling of certificates, lack of proper handling of keys within the device, as well as hard-coding keys into the application, are some of the issues related to data at rest.

3. *Lack of firmware and software updates.* The lifespan of IoT devices is quite long (up to 5–10 years). This leads to the problem of outdated software. The fact that updates in the firmware are:

- not done in an automated way;
- not transmitted in an encrypted way;
- not supported at all.

They make it possible for the system to be in use for a long time with known vulnerabilities. Moreover, the update mechanism in this case can be a threat because the update package is not protected by a digital signature. This makes it possible for the attacker to download fake firmware.

4. *Network architecture weakness and segmentation issues.* IoT devices are deployed in close proximity to other critical systems in the same network. The absence of network segmentation allows an attacker to use a compromised IoT device to access other systems in the network, thereby enabling lateral movement. This issue represents a significant threat, particularly in industrial IoT environments, which may result in stopping production in these environments.

5. *Botnet and DDoS attacks.* The high number of IoT device infections by malware results in botnet attacks. For instance, in 2016, the Mirai botnet attack caused a DDoS attack on Dyn, which temporarily restricted access to online platforms such as Twitter, Netflix, and GitHub. Therefore, IoT security affects the global internet infrastructure.

6. *Privacy and data abuse.* IoT devices collect different kinds of data about their users' daily lives, such as: geolocation data, biometrics, indoor activity data, voice commands, etc.

The lack of proper security for this data poses a significant threat to user privacy. Moreover, data transfer to third parties or use for commercial purposes may lead to ethical and legal issues. As a result of data leakage, users may be at risk of suffering different kinds of attacks, such as financial loss, identity theft, or blackmail.

7. *Physical intrusion and hardware-level attacks.* In most cases, IoT devices are installed in an uncluttered area (production area, public area, etc.). Once the attacker is able to gain physical access to the device, he can:

- Access the firmware through the JTAG and UART interfaces,
- Obtain the cryptographic keys from the memory,
- Re-program the device.

The threat of such types of attacks is critical, especially in the industrial and transportation sectors.

8. *Lack of standardization and regulation.* The IoT environment has developed without a set of standard security rules; therefore, manufacturers have a patchwork of security standards. There are some who are taking security in the IoT seriously, but some are compromising to be competitive and save money. In this case, the combination of different security standards in a network compromises the entire network.

However, IoT security is not only a technical issue but also has significant social, economic, and strategic ramifications. Today, IoT devices are involved in various aspects of life, such as smart homes and industries, healthcare, and services. The security concerns associated with IoT are not only significant for the systems but also for the overall society and people in various ways.

The level of concern regarding IoT security is substantial. IoT devices have the ability to accumulate an enormous volume of data from our daily lives. These include location information, audio, video, health information, and much

more. Because of these issues, it is entirely possible for an individual to intercept data being collected by IoT devices. In doing so, it creates an opportunity for various types of cyber crimes such as identity theft, financial crimes, privacy invasion, blackmail, and much more. A good example is an intelligent security camera and an intelligent home management system. Intercepting data from such devices is an invasion of one's personal space.

In the case of the corporate world, IoT security risks can cause more economic losses. Industrial IoT networks are connected to manufacturing, logistics, and energy management systems. An IoT cyber-attack can cause losses in the form of downtime and data losses. In 2016, the DDoS attack performed by the Mirai botnet on Dyn's services caused a shutdown of Twitter, Netflix, and GitHub services for a few hours. This is an example of how IoT security risks can cause damage to the global economic system.

In the case of the national and critical infrastructure world, the risks are more critical and can cause more damage to the system as a whole. Energy management systems, transportation systems, healthcare services, and government services are using IoT technology. In such cases, the damage caused by IoT security risks can cause more harm to the system and can even cause a threat to human life, as in the case of information loss.

In addition, security issues in IoT devices can lead to legal and ethical risks. Non-compliance with data protection legislation can result in a heavy financial penalty for companies. In addition, the unregulated collection and processing of users' information can result in a lack of public trust in companies, thereby slowing down the digital revolution.

In conclusion, the scope of security issues in IoT devices can be from individual users up to global infrastructure levels. The risks can be managed through various means: technology, legislation, standardization, and security by design. Therefore, IoT security can be viewed as a strategic issue in the information society.

Conclusion

From the analysis above, it is obvious that security issues related to IoT devices are systemic and complex. In other words, the lack of proper authentication and authorization processes, encryption issues, the absence of firmware updates, poor segmentation of the network, botnet and DDoS attacks, privacy issues, physical intrusion capability, and the lack of proper standardizations represent the main security issues of the IoT environment.

The limited availability and regulation of resources in this environment make information devices more vulnerable to criminal attacks compared to other information systems. This is not just a threat to an individual; rather, it is a problem that needs to be addressed by an organization. One good example is the Dyn DDoS attack in 2016, which was executed by a botnet called Mirai. This

attack also proves the significance of the role played by IoT in determining the worldwide internet landscape.

Based on the results obtained, it has been concluded that the security of IoT devices is not ensured only through technical means of protection. The following complex approach is crucial for the security of IoT devices.

1. The implementation of reliable methods of authentication and multi-factor authentication.

2. The application of modern methods of cryptography during data transmission and storage.

3. The application of reliable and digitally signed methods of firmware update.

4. The application of the "zero trust" approach and the segmentation of the IoT network.

5. The application of the "security by design" approach, taking into account the security issues from the design phase.

6. The improvement of international standards and mechanisms.

Therefore, it may be stated that the security aspect in the context of IoT not only involves a technical challenge but also has a number of strategic, economic, and social implications. Thus, it may be stated that in the context of a secure and sustainable growth of the IoT technology, it is not only a matter of choice but a matter of necessity for the government, industry, and the end-users to come together in order to unlock the true potential of the technology.

References

1. Weber R.H. (2010). *Internet of Things – New security and privacy challenges*. Computer Law & Security Review, 26(1), 23–30.
2. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. (2015). *Security, privacy and trust in Internet of Things: The road ahead*. Computer Networks, 76, 146–164.
3. Atzori, L., Iera, A., & Morabito, G. (2010). *The Internet of Things: A survey*. Computer Networks, 54(15), 2787–2805.
4. Roman R., Zhou J., Lopez J. (2013). *On the features and challenges of security and privacy in distributed Internet of Things*. Computer Networks, 57(10), 2266–2279.
5. Stallings W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.
6. Conti M., Dehghantanha A., Franke K., Watson S. (2018). *Internet of Things security and forensics: Challenges and opportunities*. Future Generation Computer Systems, 78, 544–546.
7. Granjal J., Monteiro E., Silva J.S. (2015). *Security for the Internet of Things: A survey of existing protocols and open research issues*. IEEE Communications Surveys & Tutorials.

Information about the authors

Gasimov V.A., Professor, Dean of the Faculty of Information and Computer Technologies, Baku Engineering University, vaqasimov@beu.edu.az.

Zahidova G.A., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, guabdullayeva@beu.edu.az.

Zeynalli-Huseynzada L.R., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, lzeynalli@beu.edu.az.

Valiyeva A.A., Assistant of Cybersecurity and Computer Engineering Department, Baku Engineering University, aveliyeva@beu.edu.az.

UDC 004.056

PROSPECTS OF USING LIGHTWEIGHT CRYPTOGRAPHY IN IoT DEVICES

Gasimov V.A., Zahidova G.A., Zeynalli-Huseynzada L.R.
Baku Engineering University, Baku, Azerbaijan

Abstract. The expansion of the IoT ecosystem necessitates a fundamental shift in securing cyber-physical systems. While security is paramount where sensors and actuators operate, resource constraints-limited memory, low throughput, and energy reserves-often make standard protocols like AES-128 technically prohibitive. This paper analyzes the transition toward Lightweight Cryptography (LWC), exploring architectural trade-offs between security margins and hardware efficiency. By evaluating optimized algorithms such as ASCON and PRESENT, the study examines their performance in constrained environments. Acknowledging current limitations, this research identifies future development paths to enhance both the performance and defensive capabilities of IoT systems.

Keywords: Lightweight cryptography; Internet of Things (IoT) security; cryptography; Advanced Standard Encryption (AES); ASCON; PRESENT; cyber-physical systems; block cipher

Introduction

With computing becoming more prevalent in people's life, they are increasingly defined by a plethora of smart gadgets or devices, Internet of Things (IoT) is one of them. Things that can communicate and interact with one another via wired or wireless transmission are referred to as IoT. These devices are time-related in that they convey information based on real-time data acquired from sensors that connect with users through a network, allowing them to take action based on their needs. IoT is a network of networked devices as shown on figure that communicate information and data in real time. The three vital main components of IoT architecture are perception layer, network layer and application layer. The physical layer, where devices such as RFID tags, sensors, and cameras assist in collecting data from the environment. The network layer, which acts as the heart of IoT as it consists of both hardware and software components and transmits information collected by the physical layer. The application layer, which serves as a link between the user and the IoT device. The devices are used in a variety of industries as:

Smart Residential Environments: In the realm of home automation, the interconnection of diverse smart devices allows for centralized management of

domestic infrastructure. Users can remotely orchestrate lighting systems, climate control, and energy consumption through mobile interfaces, achieving a seamless balance between convenience and resource efficiency.

Next-Generation Healthcare: The healthcare sector has witnessed a paradigm shift through the deployment of IoT-enabled medical sensors. By facilitating continuous, real-time physiological monitoring, these devices transmit critical patient data directly to clinical practitioners. This instantaneous feedback loop ensures that life-saving interventions can be initiated immediately upon the detection of anomalous vital signs, significantly reducing mortality rates.

Enhanced Surveillance and Public Safety: Security frameworks have been substantially fortified by networked monitoring systems. The synergy between high-definition cameras and motion sensors enables the precise tracking of assets and individuals across vast distances. This synchronized data stream, accessible via handheld devices, provides an unprecedented level of situational awareness for both private and public safety sectors.

Environmental Monitoring and Disaster Mitigation: IoT technology plays a pivotal role in catastrophe management by providing early warning systems for natural disasters. Through a distributed network of environmental sensors, vast amounts of geological and atmospheric data are analyzed to predict seismic activities or extreme weather patterns. These predictive analytics are essential for disaster preparedness, effectively minimizing human casualties and infrastructural damage.

The proliferation of Internet of Things (IoT) devices has introduced a critical challenge: the secure management of highly sensitive data, often collected autonomously without direct human intervention. In these hyper-connected environments, ensuring data integrity and preventing unauthorized access is paramount. However, the architectural reality of most IoT nodes—characterized by minimal computational throughput, restricted memory, and finite battery reserves—creates a significant barrier to traditional security implementation. These "resource-constrained" devices cannot effectively support conventional cryptographic suites such as AES, DES, or RC6, as their high-power consumption and area overhead are incompatible with the scalable and dynamic nature of IoT networks.

Furthermore, the complexity of encryption key management adds another layer of vulnerability; inadequate protocols can jeopardize the entire security framework of a lightweight system. To bridge this gap, modern scientific discourse has pivoted toward Lightweight Cryptography (LWC). These optimized algorithms are specifically engineered to strike a delicate balance between robust security margins and hardware efficiency. By mitigating the computational burden of encryption, LWC solutions offer a sustainable pathway to safeguarding privacy without compromising device performance.

This paper evaluates recent advancements in this field, comparing various block ciphers and assessing the adaptability of the Advanced Encryption Standard (AES) within the specialized constraints of the IoT domain.

Design Constraints and Security Requirements in IoT

The development of cryptographic solutions for the IoT landscape is primarily dictated by the rigorous constraints of the hardware. These devices, characterized by their compact physical dimensions, possess minimal memory (RAM/ROM) and limited computational power, yet they often require real-time responsiveness. Traditional security protocols frequently fail to meet these specific needs, leading to the emergence of Lightweight Cryptography (LWC). A qualified LWC algorithm must satisfy four fundamental security pillars: confidentiality (ensuring data is only accessible to authorized parties), integrity (preventing unauthorized alterations), authentication (verifying the identity of the communicating entities), and non-repudiation (ensuring that a transaction cannot be denied by the sender).

From an algorithmic perspective, both hardware and software efficiency are critical. In software, the focus is on reducing temporal complexity and optimizing memory footprints. In hardware, the emphasis shifts to minimizing power consumption and reducing latency – the delay between input and output – which is vital for time-sensitive IoT applications.

While both symmetric and asymmetric encryption models exist within the LWC framework, symmetric key algorithms are generally preferred for IoT designs. Asymmetric cryptography, although offering robust security, is often too computationally intensive and complex for resource-constrained nodes. In contrast, symmetric encryption provides a high-speed, low-latency alternative with significantly lower demands on storage and processing bandwidth.

Within symmetric cryptography, block ciphers have gained more traction than stream ciphers over the last decade. Their popularity stems from their versatility and the symmetry between encryption and decryption processes, which allows for the reuse of hardware components. Furthermore, block ciphers exhibit superior error propagation and diffusion characteristics, making them easier to implement in both hardware and software with minimal resource overhead. The efficacy of these ciphers is typically determined by four factors: the number of rounds, block size, key length, and the underlying architectural structure.

The internal design of a block cipher usually relies on several core mechanisms to ensure security:

Substitution-box (S-box): This component performs non-linear transformations (typically on 4-bit blocks). While S-boxes increase processing time, a higher number of active S-boxes significantly strengthens the cipher's resistance to cryptanalysis.

Permutation-box (P-box): This layer shuffles the bits to redistribute information across the block, providing the necessary bit-level diffusion.

Substitution-Permutation Network (SPN): Utilized by modern standards like AES, the SPN structure alternates between substitution and permutation layers in each round to achieve "confusion and diffusion" – the two hallmarks of secure encryption.

Iterative Rounds: Encryption is achieved through multiple rounds of these operations, with each round utilizing a unique sub-key derived from the master key.

Feistel Network: An alternative structure that divides the data into two halves, applying transformations to only one half per round before swapping them. This design simplifies the decryption process, as the same internal function can be used for both directions.

Efficiency and Attack Resistance in LWC Design

The primary objective in developing cryptographic solutions for resource-constrained hardware is to minimize the overhead across memory, silicon area, and power consumption. Optimization strategies often focus on balancing high performance with robust security. For instance, recent methodologies suggest using masking techniques – such as generating "fake keys" to hide secret keys from substitution layers – to enhance security, though this may increase the power area.

Additionally, researchers have explored methods to mitigate attack complexity by manipulating the number of iterations through related-key approaches. Specifically, in the context of AES-192, studies on reduced-round attacks indicate that the strategic placement of rounds – before rather than after the point where "impossible conditions" (cryptanalytic vulnerabilities) arise – can significantly influence the cipher's resistance to attacks. These structural refinements are essential for maintaining cryptographic strength without exceeding the strict limitations of IoT devices.

The PRESENT algorithm is a widely recognized block cipher in the LWC domain, characterized by its 64-bit block size and 80-bit key length. Research indicates that this cipher provides a robust security margin while remaining exceptionally hardware-friendly. Furthermore, implementations on FPGA (Field Programmable Gate Array) demonstrate that algorithms like Blowfish can achieve high-speed execution with minimal latency. By leveraging Hardware Description Languages (HDL) for integrated circuit design, these approaches minimize encryption time and significantly maximize system throughput, making them ideal for high-performance IoT applications.

The ASCON Cipher and the NIST LWC Standard

A significant milestone in the field of lightweight cryptography is the emergence of the ASCON family of algorithms. Designed to provide both Authenticated Encryption with Associated Data (AEAD) and hashing

capabilities, ASCON was officially selected by the National Institute of Standards and Technology (NIST) as the new standard for lightweight cryptography in 2023. This selection was primarily driven by its exceptional performance in resource-constrained environments where traditional standards like AES-GCM are inefficient.

ASCON is based on a sponge-based construction, utilizing a 320-bit permutation that balances security and throughput. It is specifically engineered to be resilient against side-channel attacks, which is a critical requirement for IoT devices deployed in physically accessible or hostile environments. The algorithm's flexibility – supporting 128-bit keys and offering various variants like ASCON-128 and ASCON-128a – allows developers to optimize for either minimum area overhead or maximum speed. By integrating ASCON into the IoT ecosystem, developers can achieve high-level data confidentiality and integrity with significantly lower power consumption and a smaller hardware footprint compared to conventional cryptographic suites.

Conclusion

The pervasive integration of IoT devices into critical sectors such as healthcare, surveillance, and disaster management underscore the urgent need for robust yet efficient security frameworks. As this research has demonstrated, traditional cryptographic standards often fail to meet the stringent power and memory requirements of resource-constrained IoT nodes. The transition toward Lightweight Cryptography (LWC) represents the most viable pathway to bridging the gap between high-level security and hardware efficiency.

Through the analysis of optimized algorithms like PRESENT and the NIST-standardized ASCON, it is evident that symmetric block ciphers and sponge-based constructions offer superior performance in constrained environments. While the adaptation of established standards like AES remains a challenge due to their inherent complexity, architectural optimizations such as S-box refining and hardware-efficient implementations provide promising results. Ultimately, the future of IoT security lies in the continued development of algorithms that provide resilience against both mathematical cryptanalysis and physical side-channel attacks. By adopting these lightweight solutions, the IoT ecosystem can achieve a sustainable balance between operational throughput and the non-negotiable requirement of data privacy.

References

1. Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J., Seurin Y., Vikkelsoe C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. International Workshop on Cryptographic Hardware and Embedded Systems. Springer. 4727, 450–466.

2. Dobraunig C., Eichlseder M., Mendel F., Schl  ffer M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology. Springer. 34 (3), 1–42.
3. Menezes A. J., Van Oorschot P. C., Vanstone S. A. (2018). Handbook of Applied Cryptography. CRC Press. 5th Edition, 191–220.
4. Daemen J., Rijmen V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. Information Security and Cryptography. Springer. 1, 31–55.
5. Hatzivasilis G., Fysarakis K., Papaefstathiou I., Papadakis C. (2018). A Review of Lightweight Block Ciphers. Journal of Cybersecurity and Information Management. Elsevier. 2 (1), 15–32.
6. NIST. (2023). NIST Selects ‘Ascon’ Algorithms for Lightweight Cryptography. National Institute of Standards and Technology. NIST News (Special Publication), 800–175.
7. Rolfes C., Poschmann A., Paar C. (2008). Ultra-Lightweight Implementations for Smart Devices – Is PRESENT Enough? International Conference on Smart Card Research and Advanced Applications. Springer. 5189, 247–262.
8. Guo J., Peyrin T., Poschmann A., Robshaw M. (2011). The PHOTON Family of Lightweight Hash Functions. International Cryptology Conference. Springer. 6841, 222–239.

Information about the authors

Gasimov V.A., Professor, Dean of the Faculty of Information and Computer Technologies, Baku Engineering University, vaqasimov@beu.edu.az.

Zahidova G.A., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, guabdullayeva@beu.edu.az.

Zeynalli-Huseynzada L.R., Lecturer of Cybersecurity and Computer Engineering Department, Baku Engineering University, lzeynalli@beu.edu.az.

УДК 004.056.5

АЛГОРИТМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ

¹И.Х.Норматов, ²Р.Н.Дадажанов, ³М.Н.Атаджанов,

¹*Национальный университет Узбекистана имени Мирзо Улугбека,
Ташкент, Узбекистан*

²*Университет общественной безопасности Республики Узбекистан,
Ташкент, Узбекистан*

³*Военно-академический лицей имени Джалолиддина Мангуберди, Ургенч,
Узбекистан*

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности систем обработки и хранения конфиденциальной информации. Предлагается алгоритмическая модель анализа защищенности информационных систем на основе динамических таблиц функционирования. Рассматриваются особенности управления и контроля потоков данных, а также методы оценки уровня защиты информационных ресурсов. Алгоритмическая модель используется как математический аппарат для моделирования динамических дискретных систем и позволяет выявлять уязвимости в функционировании системы защиты. Применение предложенного подхода обеспечивает более эффективное исследование состояния информационной

безопасности и повышение надежности систем защиты конфиденциальной информации.

Ключевые слова: информационная безопасность, защита конфиденциальной информации, алгоритмическая модель, таблицы функционирования, информационные системы, анализ защищенности, динамические системы, обработка данных, безопасность информации.

ALGORITHMIC MODEL OF INFORMATION SECURITY BASED ON FUNCTIONING TABLES

¹I.Kh. Normatov, ²R.N. Dadazhanov, ³M.N. Atadzhanov

¹*National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan*

²*University of public safety of the republic of Uzbekistan, Tashkent, Uzbekistan*

³*Military academic lyceum named after Jaloladdin Manguberdi, Urgench, Uzbekistan*

Abstract. Ensuring the security of information systems that process and store confidential data is an important task in modern digital infrastructures. This paper presents an algorithmic model of information security based on functioning tables. The proposed approach allows the formal description of information processes and the analysis of system states in the context of security control. Functioning tables are used as a mathematical tool for modeling the behavior of dynamic discrete systems and evaluating the effectiveness of security mechanisms. The developed model makes it possible to analyze information flows, identify potential vulnerabilities, and assess the reliability of protection mechanisms in information systems. The results of the study demonstrate that the use of functioning tables improves the efficiency of security analysis and provides a systematic approach to the protection of confidential information.

Keywords: information security, algorithmic model, functioning tables, confidential information protection, information systems, security analysis, data flow control.

Введение

Развитие информационных систем обработки и хранения конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

В данной работе рассматриваются особенности работы с потоками данных, управление и контроль над ними, приводятся математические решения оценки защиты информационных ресурсов и различные аспекты оценивания экономической эффективности обеспечения конфиденциальности информационных ресурсов. Предлагается один из способов анализа защищенности системы – построение динамических таблиц функционирования (ТФ) информационной системы. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализуемой системы защиты, и выявляются ее недостатки. В работе алгоритмические модели на основе ТФ используются

как математический аппарат для моделирования динамических дискретных систем [1–8].

Безопасность – это отсутствие опасности или наличие возможности надежно защититься от нее. Опасным следует считать такое информационное воздействие, которое чревато дестабилизирующим, деструктивным, ущемляющим интересы личности или страны и т.д. результатом.

Информационная безопасность общества, государства – это состояние либо отсутствия информационных угроз, либо, при наличии таковых, состояние защищенности и, следовательно, устойчивости основных сфер жизнедеятельности (политики, экономики, науки, техносферы, сферы государственного управления, культуры, военного дела, общественного сознания и т.д.) по отношению к опасным информационным воздействиям, причем как внедрению, так и извлечению информации.

Системный подход к информационной безопасности (ИБ) требует выделять ее субъекты, средства и объекты, принципы обеспечения, источники опасности, направленность опасных информационных потоков.

Эволюция информационных технологий (ИТ) связана с интеллектуальными системами, в которых присутствуют процессы зарождения, адаптации и развития. Системный подход определяет методологию и принципы построения систем ИТ. Принцип возможности моделирования позволяет предотвратить ошибки проектирования кибернетических систем. Принцип связности при разработке эффективной системы рассматривает объект защиты комплексно, объединяя объект защиты, внешнюю среду, средства защиты и угрозы злоумышленника и учитывая взаимосвязи: источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).

Построение системы защиты является обязательным условием для обеспечения безопасности конфиденциальной информации, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы является построение динамических таблиц функционирования (ТФ) информационной системы на базе сетей Петри [20]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Развитие информационных систем обработки и хранения

конфиденциальной информации диктует необходимость построения надежной системы защиты конфиденциальной информации (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование информационной системы (ИС), в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности конфиденциальной информации (КИ), а также составляются требования к СЗКИ.

Требования к СЗКИ, в зависимости от вида КИ определяются согласно нормативно-законодательной базы Республики Узбекистан.

Алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем

Моделирование на основе ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнение событийной модели в ТФ описывает поведение системы. На основе анализа результатов выполнения можно сказать о возможных состояниях системы, и при этом какие состояния в принципе не достижимы.

Основная часть

Таким образом, $ТФ = \{X, Y, A, O, \Theta, T, U, S, F, P\}$ – алгоритмическая модель АСУ обеспечения безопасности ИС, а также предотвращения любого вида угроз к ИС и информационным ресурсам (ИР), где

Y – множество возможных угроз O_j , $Y = \{O_j\}$;

X – множество решений предотвращения угроз A_i , $X = \{A_i\}$;

A – определенное решение предотвращения угроз;

O – определенное действие угроз;

Θ – множество координат Θ_{ij} соответствия A_i и O_j , $\Theta = \{\Theta_{ij}\}$;

T – время предотвращения и успешной реализации угрозы;

U – внешнее воздействие на $\{A_i; O_j\}$ по координате Θ_{ij} ;

S – множество переходов S_{ij} (переход из одной Θ_{ij} на другую $\Theta_{i+n, j+m}$);

$F(t)$ – функция изменения таблицы функционирования во времени;

P – множество вычислительных и логических операций ввода, вывода и управления;

Z – множество привилегий.

Если $\forall t_i \in T$ функция $F(t_i) = \text{const}$, то такая таблица функционирования называется статической (стационарной). Функция $F(t)$, задающая

изменения таблицы функционирования, называется функцией управления агрегатной системой или функцией планирования процессов в системе.

В каждый интервал времени t_i описание ТФ представляется в виде маркированной сети Петри: $M = \{P, D, I, O, \mu\}$, где P, D, I, O - соответственно, множества позиций (состояний), операций (переходов), входных и выходных состояний; μ -функция, отображающая множество позиций в множество натуральных чисел $N: \mu: P \rightarrow N$. Каждая маркировка μ может быть представлена как вектор $\mu = (\mu_1, \dots, \mu_n)$, здесь $n = |P| \forall \mu_i \in N, i = \overline{1, n}$. Вектор μ определяет для каждой позиции P_i сети количество фишек, т.е. для $\mu_i, P_i, i = \overline{1, n}$ выполняется $\mu(P_i) = \mu_i$. Интервалы времени, в течение которых сеть Петри не изменяется, будем называть технологическими циклами (ТЦ) [1,3].

Таким образом, за неделимый элемент динамических дискретных систем принято рабочее место (РМ), соответствующее α_i определенному решению предотвращения угроз. Обозначим его через α_i , а множество РМ - через A . Каждое α_i может быть представлено в виде работников, работника плюс машины или машины. Каждое α_i имеет входы x и выходы y , внутреннее z состояние. На входы передаются сигналы (информация) или материалы в виде продуктов, веществ (жидких или газообразных) и т. д. Некоторые входные воздействия сигналов могут быть управляющими (g). В качестве машин применяются станки и вычислительные машины. Машины выступают в качестве орудия труда, а информация, материалы – в качестве предметов труда.

Рабочее место α_i соответствует агрегату Н.П. Бусленко. Каждому агрегату приписывается определенное количество операций d . Множество операций α_i обозначим через D . Кроме того, они функционируют во времени и имеют пространственные координаты. Множество РМ соединяются между собой дугами и образуют коммуникационную сеть с потоками α (имеется в виду потоки информации, веществ, а также транспортные, людские потоки и т.д.).

Так, система представляется в виде коммуникационной сети, вершины которой изображают РМ, способные выполнять определенное количество операций (решение задач, переработка материалов и т.д.), а дуги соответствуют потокам между этими местами. Таковую сеть назовем R -сетью.

В процессе функционирования системы структура сети со временем может меняться: старые дуги и вершины аннулируются, а новые добавляются. Такие сети назовем ситуационными или RC -сетями. При решении определенного класса задач в течение времени (t_1, t_2) на каждом α выполняется одна из приписанных ему операций. Поэтому построение

самой сети и определение приписанной операции является основной задачей системных исследований. В определенный промежуток времени сеть можно изобразить в виде ориентированного графа неизменной структуры (рис. 1). Такое представление соответствует определению таблицы функционирования, и R -, RC сети представляются в виде ТФ. На этой сети можно фиксировать параметры потока и режим работы сети во времени [1, 2].

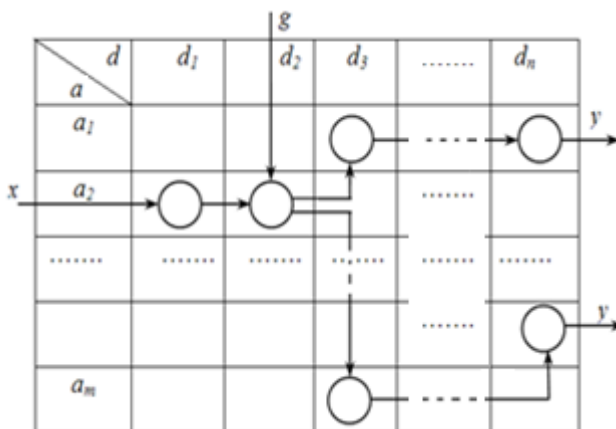


Рис. 1. ТФ гипотетического объекта управления
Fig. 1. TF of a hypothetical control object.

Воспользуясь системами действий сетей Петри мы создадим блок схему СЗКИ (рис. 2) и гибридный вариант сетей Петри в обеспечении ИБ. В блок схеме основным шагом является обнаружение угрозы O_j из множества Y . После идентификации угрозы O_j она проверяется общим архивом (П+И) просмотренных угроз. Если такие угрозы были рассмотрены ранее они обезвреживаются соответственными действиями $\{P_{ij} F\}$. Если угроза рассматривается впервые тогда она анализируется и вычисляется $\{Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i\}$. Если после анализа источника $Y+Z$ и анализа привилегии Z_k угрозы не обнаружатся тогда они пересматриваются как $Y+Z_k$. После этого добавляются в архив пропущенных угроз П. Если при анализе и вычислении угрозы обнаружатся, то тогда действия будут идти по блок схеме № 1, Продолжение. Здесь после всех шагов угрозы добавляются в архив для быстрого обнаружения и идентификации угроз (рис. 2).

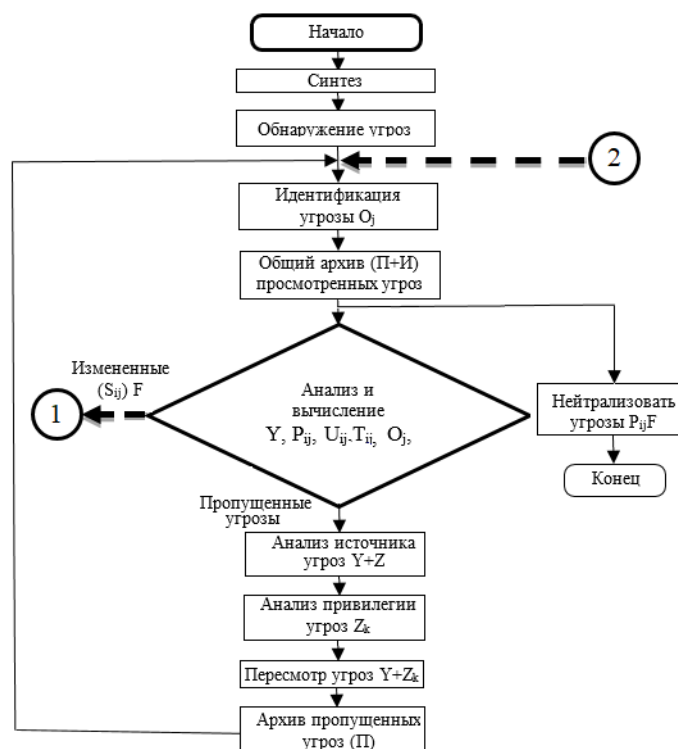


Рис. 2. Алгоритм работы ТФ № 1 (продолжение)

Fig. 2. Tables of functioning operation algorithm No. 1 (continued)



Рис. 3. Схема построения алгоритмической модели СКЗИ на основе ТФ

Fig. 3. The scheme of constructing an algorithmic model of the means of confidential information protection based on tables of functioning

На рис. 3 в таблице функционирования представлены множество угроз $\{O_j\}$, а также множество действий $\{A_i\}$ для предотвращения угроз. Для функционирования данной ТФ необходимо в каждой ячейке было предоставлено минимум 3 входа: сама угроза; способы предотвращения

данной угрозы; привилегия пользователя в данной ситуации (например – системный администратор и пользователи разных уровней).

После обработки действия в ячейке ($A_2 O_2$) по формуле $\theta_{ij} = \{Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i, Z_k\}$ состояние угрозы меняется исходя из своей сущности и скрипта кода, после этого управление передается в другую ячейку. В нашем случае в (A_3, O_3). Переход осуществляется по формуле $\{S_{ij}, F\}$.

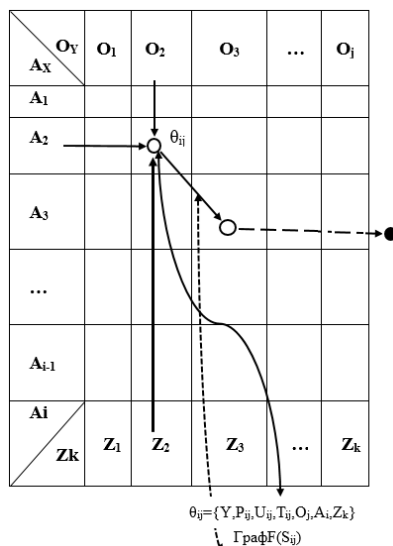


Рис. 4. Таблица функционирования СЗКИ

Fig. 4. Table of functioning the means of confidential information protection

После окончания обработки угроза выводится из таблицы, т.е. уничтожается или добавляется в архив. При этом нужно учитывать то, что алгоритм работы ТФ № 1 является гибким и всегда может изменяться при обработке данных и будет совершенствоваться. Это отразится и на ТФ, которая будет постоянно дополняться новыми критериями. Эти действия в сетях Петри представлены в таблице на рис. 4.

Анализируя вышеотмеченные выводы и полученную таблицу функционирования, можно сконструировать для определенной внешней угрозы на систему пути вычисления, анализа и график работы в предлагаемой нами сети СЗКИ.

Заключение

Предложена алгоритмическая модель информационной безопасности на основе таблиц функционирования. Алгоритмический метод на основе таблицы функционирования использован как математический аппарат для моделирования динамических дискретных систем обнаружения и обезвреживания угроз при обеспечении защиты информации. Разработан метод оценки рисков информационной безопасности и обеспечения конфиденциальности информационных ресурсов. Предложен один из способов анализа защищенности системы – построение динамических

таблиц функционирования. Предложены математические решения оценки защиты информационных ресурсов и различные аспекты оценивания экономической эффективности обеспечения конфиденциальности информационных ресурсов.

Список использованных источников

1. Питерсон Дж. Теория сетей Петри и моделирование систем. М.: Мир, 1984.
2. Пospelов Г.С. Системный анализ и искусственный интеллект// Проблемы вычислительной техники. М.: Международный центр науки и техн. информ., 1981. С. 21–42.
3. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. М.: Физматлит, 2001.
4. Кабулов А.В. Норматов И.Х., Каландаров И.И. Алгоритмический подход управления сложными системами на примере производственных систем // ДАН АН РУз, г.Ташкент. 2017. № 1. С. 33–35.
5. Kabulov A.V., Normatov I.X., Kalandarov I.I., Karimov A.A. Algorithmic Method of Organization of Specialized Workshops // International Journal of Advanced Research in Science, Engineering and Technology. 2018. Vol. 5, iss. 4. P. 5670–5675.
6. Норматов И.Х. Алгоритм обнаружения и обезвреживания угроз на основе таблиц функционирования // IV Международный Косыгинский Форум «Проблемы инженерных наук: формирование технологического суверенитета». Сборник научных трудов Международного научно-технического симпозиума «Современные инженерные проблемы ключевых отраслей экономики страны» (20–22 февраля 2024 г.). Том 1. М.: РГУ им. А.Н. Косыгина, 2024. С. 78–84.
7. Норматов И.Х., Атажанов М.Н. Эффективность применения искусственного интеллекта (Artificial intelligence (AI)) в образовательном процессе // International scientific and practical Conference of students, undergraduates, doctoral students and young scientists «Student, science and Innovation: modern research trends» dedicated to the Day of Science workers and the 125th anniversary of Kanysh Satpayev, 10 April 2024.
8. Normatov I., Atazhanov M., Karimov R. Development of an algorithmic system for detecting and disarming threats based on functioning tables // Технические средства защиты информации: материалы XXIII Международной научно-технической конференции, Минск, 08 апреля 2025 года / Белорусский государственный университет информатики и радиоэлектроники [и др.]; редкол.: О. В. Бойправ [и др.]. Минск, 2025. С. 22–26.

References

1. Peterson J. Petri Net Theory and Systems Modeling. Moscow: Mir, 1984. (In Russian)
2. Pospelov G.S. Systems Analysis and Artificial Intelligence// Problems of Computer Engineering. Moscow: International Center for Science and Technical Information, 1981. pp. 21–42. (In Russian)
3. Samarskii A.A., Mikhailov A.P. Mathematical Modeling: Ideas. Methods. Examples. Moscow: Fizmatlit, 2001. (In Russian)
4. Kabulov A.V., Normatov I.Kh., Kalandarov I.I. An Algorithmic Approach to Controlling Complex Systems Using Production Systems as an Example // DAN AS RUz, Tashkent. 2017. No. 1. pp. 33–35. (In Russian)
5. Kabulov A.V., Normatov I.Kh., Kalandarov I.I., Karimov A.A. Algorithmic Method of Organization of Specialized Workshops // International Journal of Advanced Research in Science, Engineering and Technology. 2018. Vol. 5, iss. 4. P. 5670–5675.

6. Normatov I.Kh. Algorithm for detection and neutralization of threats based on functioning tables // IV International Kosygin Forum "Problems of Engineering Sciences: Formation of Technological Sovereignty". Collection of scientific papers of the International Scientific and Technical Symposium "Modern Engineering Problems of Key Branches of the Country's Economy" (February 20–22, 2024). Vol. 1. Moscow: A.N. Kosygin State University, 2024. P. 78–84. (In Russian)

7. Normatov I.Kh., Atazhanov M.N. The effectiveness of using artificial intelligence (AI) in the educational process // International scientific and practical Conference of students, undergraduates, doctoral students and young scientists "Student, science and Innovation: modern research trends" dedicated to the Day of Science workers and the 125th anniversary of Kanysh Satpayev, April 10, 2024. (In Russian)

8. Normatov I., Atazhanov M., Karimov R. Development of an algorithmic system for detecting and disarming threats based on functioning tables // Technical means of information protection: Proceedings of the XXIII International Scientific and Technical Conference, Minsk, April 8, 2025 / Belarusian State University of Informatics and Radioelectronics [et al.]; ed. board: O. V. Boiprav [et al.]. Minsk, 2025. pp. 22–26.

Информация об авторах

Норматов И.Х., доктор физико-математических наук, профессор, директор Научно-инновационного центра «Цифровые технологии и кибербезопасности» имени академика В.К.Кабулова при Национального университета Узбекистана имени Мирзо Улугбека i_normatov@nuu.uz.

Дадажанов Р.Н., кандидат физико-математических наук, доцент Университета общественной безопасности Республики Узбекистан, Ташкент, Узбекистан dadajonovrn@mail.ru.

Атажонов М.Н., преподаватель Военно-академического лицея имени Джалалуддина Мангуберди, muzaffar19910627@gmail.com.

Information about the author

Normatov I.Kh., Doctor of Physical and Mathematical Sciences, Professor, Director of the Scientific and Innovation Center "Digital Technologies and Cybersecurity" named after Academician V.K. Kabulov at the National University of Uzbekistan named after Mirzo Ulugbek, i_normatov@nuu.uz.

Dadazhanov R.N., Candidate of Physical and Mathematical Sciences, Associate Professor, University of Public Security of the Republic of Uzbekistan, Tashkent, Uzbekistan, dadajonovrn@mail.ru.

Atadzhanov M.N., Lecturer, Military Academic Lyceum named after Jalaluddin Manguberdi, muzaffar19910627@gmail.com.

УДК 003.26

ОБОБЩЕННАЯ МОДЕЛЬ ИЕРАРХИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С РАСПРЕДЕЛЕННЫМ РЕЕСТРОМ В ЦИФРОВОЙ СРЕДЕ УПРАВЛЕНИЯ ГОСУДАРСТВОМ

А.М. Макаров, Е.А. Писаренко, Б.М. Гаджимурадов
*ФГБОУ ВО «Пятигорский государственный университет»,
г. Пятигорск, Россия*

Аннотация. В статье представлена обобщенная модель иерархической информационной системы с распределенным реестром на основе блокчейн-технологии для цифровой среды управления государством. Рассмотрена трехуровневая архитектура системы: федеральный, региональный и муниципальный уровни. Описан протокол включения новых блоков в одноранговую блокчейн-цепь с механизмом достижения консенсуса. Предложенная модель обеспечивает криптографически-технологическое доверие между абонентами всех уровней системы при создании электронных государственных услуг и сервисов.

Ключевые слова: блокчейн-технология; распределенный реестр; иерархическая информационная система; цифровое государство; электронные государственные услуги; консенсус; криптографическое доверие; одноранговая сеть; цифровая среда; государственное управление.

GENERALIZED MODEL OF A HIERARCHICAL INFORMATION SYSTEM WITH DISTRIBUTED LEDGER FOR DIGITAL GOVERNMENT MANAGEMENT

A.M. Makarov, E.A. Pisarenko, B.M. Gadzhimuradov
Pyatigorsk State University, Pyatigorsk, Russia

Abstract. A generalized model of a hierarchical information system with distributed ledger based on blockchain technology for digital government management is presented. A three-level system architecture is considered: federal, regional, and municipal levels. The protocol for including new blocks in the peer-to-peer blockchain with a consensus mechanism is described. The proposed model provides cryptographic-technological trust between subscribers at all system levels when creating electronic government services and applications.

Keywords: blockchain technology; distributed ledger; hierarchical information system; digital state; electronic government services; consensus; cryptographic trust; peer-to-peer network; digital environment; public administration.

Введение

Создание электронных государственных услуг и сервиса, обеспеченного доверительной средой интеграции друг с другом – это первостепенная задача любого общества, вступающего в цифровое пространство. В государстве, функционирующем в цифровой среде,

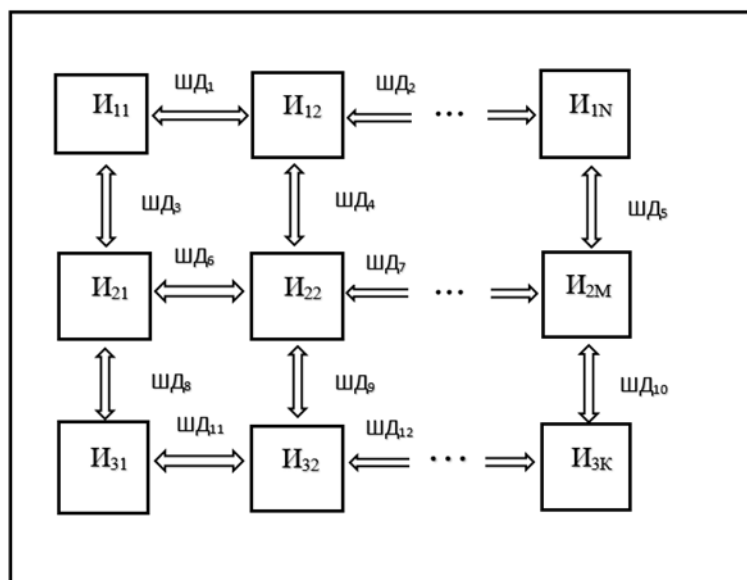
государственные информационные системы (ГИС), обладают приоритетным правом. Уже на их базе, будет выстраиваться система для региональных (округа, области) и муниципальных органов власти. ГИСы должны будут ускорить создание электронных государственных сервисов, упростить их интеграцию. Основное назначение ГИС верхнего уровня: в информационном поле ГИС должна обеспечиваться слаженная работа всех встроенных систем, как по вертикали, так и по горизонтали с гарантированным доверием друг к другу.

Технологией, которая решит задачу обеспечения гарантированного доверия абонентов всех уровней, является «блокчейн-технология», которая реализуется в системах с распределенным реестром и обеспечит криптографически – технологическое доверие в цифровом обществе.

Основная часть

В основе вышеуказанной технологии, в свою очередь, лежит технология асимметричного криптографического шифрования и порождаемые ею технологии криптографического хэширования, цифровой подписи и токенизации процессов.

Обобщенная модель иерархической информационной системы с распределенным реестром (блокчейн технология) цифровой среды Российской Федерации представлена на рисунке.



Модель иерархической информационной системы с распределенным реестром
(блокчейн технология) цифровой среды РФ
A model of a hierarchical information system with a distributed registry (blockchain
technology) of the digital environment of the Russian Federation

На рисунке обозначено:

I_{1N} – информационная, состоящая из N систем верхнего (государственного) уровня

I_{2M} – информационная, состоящая из M систем среднего (краевого, областного, окружного) уровня

I_{3K} – информационная, состоящая из K систем нижнего (муниципального) уровня

$ШД_1, ШД_2, \dots, ШД_N$ – шины данных верхнего уровня

$ШД_6, ШД_7, \dots, ШД_M$ – шины данных среднего уровня

$ШД_{10}, ШД_{11}, \dots, ШД_K$ – шины данных нижнего уровня

$ШД_3, ШД_4, ШД_5$ – шины данных, связывающие верхний и средние уровни

$ШД_8, ШД_9, ШД_{10}$ – шины данных, связывающие средний и нижний уровни

Протокол работы сети распределенного реестра (блокчейн технологии) информационной системы при включении вновь созданного блока в одноранговую блокчейн цепь (ОБЧЦ)

Исходные условия:

НК имеет открытые ключи всех абонентов всех подсистем распределенного реестра: $K_1, K_2, \dots, K_n$.

Открытый ключ НК – КНК известен всем n -абонентам. Закрытые ключи строго хранятся у всех абонентов и НК.

Цель: Абонент A_1 хочет включить вновь созданный им блок в ОБЧЦ.

A_1 сообщает НК о включении блока с данными D_1 в ОБЧЦ:

$A_1 \rightarrow НК : \{A_1, D_1, h_1\}_{(K_{НК})}$,

где h_1 – хэш функция нового блока, созданная A_1 .

НК получает сообщения от A_1 , устанавливает и верифицирует его. Получив блок, НК по h_1 и хэш функции предыдущего блока вычисляет новую хэш функцию нового блока и включает его в ОБЧЦ с меткой текущего времени. (можно ли с меткой текущего времени) После чего рассылает этот блок i -тым абонентам соответствующего распределенного реестра.

$НК \rightarrow A_i : \{A_1, D_1\}_{(K_i)}$, $i=1, 2, \dots, N_1$, где N_1 – число абонентов распределенного реестра, участвующих в процессе достижения консенсуса о правомерности включения нового блока в ОБЧЦ.

Через установленный интервал времени НК может получить следующие ответы абонентов распределенного реестра:

Консенсус достигнут, возражений нет. Тогда НК приводит корректировку истории времени включения блока в ОБЧЦ и дает команду абонентам распределенного реестра о включении блоков в базу данных всех абонентов.

При появлении возражения у одного или нескольких абонентов, блок отсылается на доработку. Если все абоненты согласовали свое

положительное мнение, то история достижения согласия (временная отсечка) не корректируется и все возникшие вопросы вносятся в новый блок: какой и от кого вопрос (данные абонентов должны быть обезличены). Далее, следует команда НК о включение нового блока в базу данных абонентов распределенного реестра.

Заключение

В предлагаемой модели, многофункциональную роль НК сложно переоценить. В случае, отсутствия консенсуса и необходимости вмешательства, НК корректируют время передачи блока на арбитраж, вносит вопросы, вызвавшие возражения, в блок и помечает данный блок как спорный.

Список использованных источников

1. Гаджимурадов Б.М., Макаров А.М. Иерархическая многоуровневая система распределенного реестра (блокчейн технология) контроля целостности данных при разработке, распределении, целевом использовании финансового бюджета. Заявка (30.12.2025); Регистрационный № 2025139803 в Федеральной службе по интеллектуальной собственности (59 с.).

References

1. Gadzhimuradov B.M., Makarov A.M. Hierarchical multilevel distributed registry system (blockchain technology) for data integrity control in the development, distribution, and targeted use of the financial budget. Application (12/30/2025); Registration number 2025139803 in the Federal Service for Intellectual Property (59 pages).

Сведения об авторах

Гаджимурадов Б.М., канд. эконом. наук, доц. каф. ИКТМИБ ФГБОУ ВО «Пятигорский государственный университет», *baxa78@bk.ru*;

Макаров А.М., д-р техн. наук, проф. каф. ИКТМИБ ФГБОУ ВО «Пятигорский государственный университет», *mellin_22@mail.ru*;

Писаренко Е.А., канд.пед.наук, доц., доц. каф. ИКТМИБ ФГБОУ ВО «Пятигорский государственный университет»

Information about the authors

Gadzhimuradov B.M., PhD in Economics, associate professor at the Department ICTMSB, “Pyatigorsk State University”, *baxa78@bk.ru*;

Makarov A.M., doctor of Technical Sciences, Professor at the Department ICTMSB “Pyatigorsk State University”, *mellin_22@mail.ru*;

Pisarenko E.A., PhD in Pedag., Associate Professor at the Department of ICTMSB “Pyatigorsk State University”;

СТАТЬИ ПО МАТЕРИАЛАМ СЕКЦИОННЫХ ДОКЛАДОВ ARTICLES BASED ON THE MATERIALS OF SECTIONAL REPORTS

УДК 004.9

БЕЗОПАСНОСТЬ ДАННЫХ В СПОРТИВНЫХ ПРИЛОЖЕНИЯХ

С.А. Зайкова

*Учреждение образования «Гродненский государственный университет
имени Янки Купалы», г. Гродно, Республика Беларусь*

Аннотация. Рассмотрены практические методы, используемые при разработке комплексного подхода к защите и шифрованию данных в мобильных приложениях, включая спортивное направление. Исследованы угрозы, с которыми сталкиваются разработчики подобных приложений, а также создание эффективных мер по обеспечению конфиденциальности, целостности и доступности данных пользователей.

Ключевые слова: мобильное приложение; защита данных; шифрование; угрозы безопасности; персональные данные.

DATA SECURITY IN SPORTS APPS

S. Zaikova

*Educational Institution “Yanka Kupala State University of Grodno”, Grodno,
Republic of Belarus*

Abstract. This article examines practical methods used in developing a comprehensive approach to protecting and encrypting data in mobile apps, including those in the sports sector. It explores the threats faced by developers of such apps, as well as the development of effective measures to ensure the confidentiality, integrity, and availability of user data.

Keywords: mobile application; data protection; encryption; security threats; personal data.

В наше время новых возможностей, которые предоставляют пользователям современные спортивные и фитнес приложения, приходят и новые вызовы, особенно в контексте защиты личных данных. В мире, где цифровые следы наших действий становятся все более яркими и запутанными, защита персональной информации становится крайне важной, а ее утечка или использование в противоправных целях могут иметь серьезные последствия для нашей частной жизни [1, 2].

Спортивные приложения предоставляют уникальные возможности для отслеживания физической активности, анализа тренировок, и обмена опытом с сообществом единомышленников. Однако, с ростом популярности этих приложений возрастает и необходимость обеспечения их безопасности и защиты данных пользователей.

Проблема безопасности в спортивных мобильных приложениях становится все более актуальной, поскольку они хранят и обрабатывают чувствительные личные данные [3]. Пользователи доверяют такого рода приложениям свои персональные данные, связанные со здоровьем.

Разработчику необходимо предусмотреть не только интуитивно понятный интерфейс приложения, но и обеспечить высокий уровень конфиденциальности этой информации.

Несанкционированный доступ к данным пользователя может привести к серьезным последствиям, таким как: утечка персональных данных, медицинской истории и результатов тренировок. Кроме того, некорректная передача данных через сеть может привести к их перехвату.

Психологический аспект: утечка личных данных в сфере здоровья и физической активности может повлечь за собой эмоциональные и психологические последствия для пользователя, нарушая его чувство конфиденциальности и безопасности. Доверие пользователей: утечка данных может серьезно подорвать доверие пользователей к приложению и специалистам, разработавшим приложение.

Эффективная защита от утечки личных данных в спортивных мобильных приложениях требует комплексного подхода, включая использование современных методов шифрования, строгие политики доступа, регулярное тестирование безопасности и обучение пользователей основам безопасности.

Разработанное программное решение предусматривает следующие шаги: регистрация (ввод логина и пароля), ввод личных данных (название аккаунта, имя, возраст, место проживания), шифрование данных с помощью соли, внос в базу данных уже зашифрованные данные (хэш и соль). Затем пользователь мобильного приложения может проверить свои данные (вводит логин и пароль, если все верно, то данные дешифруются из базы данных и выводятся).

В начале программы пользователь выбирает, что ему надо сделать (проверить регистрацию и получить данные или зарегистрироваться). Затем выполняется проверка на правильность выбора, после чего пользователь вводит данные для регистрации в приложении. Демонстрация шифрования данных приведена на рис. 1.

Алгоритм AES является одним из самых широко используемых алгоритмов симметричного шифрования. Он обеспечивает высокую степень безопасности при относительно высокой скорости выполнения операций. AES использует блоки фиксированной длины (128 бит) и ключи различной длины (128, 192 или 256 бит).

Отметим, что защита персональных данных пользователя в базе крайне важна. При разработке прототипа предложено шифровать данные с помощью алгоритмов шифрования и соли. Злоумышленник, который получит данные, будет видеть только хэш, который он не сможет использовать. Чувствительные данные останутся в безопасности.

В результате проведенной работы выполнен анализ уязвимостей и угроз безопасности приложения, включая outline, разработаны

и применены некоторые методы шифрования данных. Практическая реализация предложенных мер безопасности реализована в прототипе спортивного мобильного приложения. Разработаны рекомендации конечным пользователям такого рода приложений с целью повышения их осведомленности в вопросах безопасности персональных данных.

```
// Generate a unique salt for each user field
byte[] passwordSalt = GenerateSalt();
byte[] nameSalt = GenerateSalt();
byte[] ageSalt = GenerateSalt();
byte[] residenceSalt = GenerateSalt();

// Encrypt user data
string encryptedPassword = AesEncryptionHelper.EncryptData(password,
passwordSalt);
string encryptedName = AesEncryptionHelper.EncryptData(name, nameSalt);
string encryptedAge = AesEncryptionHelper.EncryptData(age, ageSalt);
string encryptedResidence = AesEncryptionHelper.EncryptData(residence,
residenceSalt);

// Save user to database
RegisterUser(username, encryptedPassword, encryptedName, encryptedAge,
encryptedResidence, Convert.ToBase64String(passwordSalt),
Convert.ToBase64String(nameSalt), Convert.ToBase64String(ageSalt),
Convert.ToBase64String(residenceSalt));

}
```

Шифрование данных в приложении
Encrypting data in the application

Список использованных источников

1. Меры по обеспечению защиты персональных данных: учебное пособие / А. И. Гавриленко [и др.]; под общ. ред. А.А. Гаева, М.А. Городецкой. – Минск: РИВШ, 2025. – 78 с.
2. Защита персональных данных : учебное пособие / А.А. Гаев. [и др.]; под. общ. ред. М.Г. Коршекевича, М.А. Городецкой. – Минск: РИВШ, 2024. – 124 с.
3. Зайкова С.А. Обеспечение безопасности процесса аутентификации с использованием дополнительных факторов / С. А. Зайкова // Технические средства защиты информации: матер. XXIII Междунар. науч.-техн. конф., Минск, 8 апр. 2025 г. – Минск: БГУИР, 2025. – С. 161–164.

References

1. Measures to Ensure the Protection of Personal Data: A tutorial / A.I. Gavrilenko, [et al.]; edited by A.A. Gaev, M.A. Gorodetskaya. Minsk: RIVSh, 2025. – 78p.
2. Personal Data Protection: A tutorial / A.A. Gaev, [et al.]; edited by M.G. Korshekevich, M.A. Gorodetskaya. Minsk: RIVSh, 2024. – 124p.

3. Zaikova S.A. Ensuring the Security of the Authentication Process Using Additional Factors / S.A. Zaikova // Technical Means of Information Protection: Proc. of the XXIII Int. Scientific and Technical Conf., Minsk, April 8, 2025. – Minsk: BSUIR, 2025. – P. 161–164.

Сведения об авторе

Зайкова С.А., канд. физ.-мат. наук, доц., доцент кафедры СПиКБ, учреждение образования «Гродненский государственный университет имени Янки Купалы», sunny@mf.grsu.by.

Information about the author

Zaikova S., Cand. Sci. (Phys. and Math. Sciences), Associate Professor, Department Lecturer, Educational Institution “Yanka Kupala State University of Grodno”, sunny@mf.grsu.by.

УДК 004.056.5:006.89

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ СТБ ISO/IEC 27001-2024 В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С.Ю. Воробьёв, Е.А. Ханчевский

*Научно-исследовательское и проектно-изыскательское республиканское
унитарное предприятие «Белэнергосетьпроект», г. Минск,
Республика Беларусь*

Аннотация. Процессы цифровой трансформации энергетической отрасли служат триггером для осуществления комплекса мероприятий по защите информации, обрабатываемой в информационных системах организаций и предприятий белорусской энергетики. Вместе с тем вопросы эффективности результатов внедрения требований стандарта СТБ ISO/IEC 27001-2024 в операционную деятельность последних остаются практически неизученными как на уровне научной среды, так и работников производственной сферы. В статье приведен кейс по внедрению системы менеджмента информационной безопасности в деятельность одного из предприятий, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь с интерпретацией полученных результатов.

Ключевые слова: энергетика; информационная безопасность; защита информации; системы менеджмента; стандарты; сертификация; кибербезопасность, риски информационной безопасности; 27001.

IMPLEMENTATION OF STB ISO/IEC 27001-2024 REQUIREMENTS IN THE ACTIVITIES OF AN ENERGY INDUSTRY ENTERPRISE

S.Yu. Vorobyov, E.A. Khanchevsky

*Belenergoproekt, a research and development and design and survey
republican unitary enterprise, Minsk, Republic of Belarus*

Abstract. The digital transformation of the energy sector is triggering a series of measures to protect information processed in the information systems of Belarusian energy

organizations and enterprises. However, the effectiveness of implementing the requirements of the STB ISO/IEC 27001-2024 standard in the operations of these organizations remains largely unexplored, both by the scientific community and by industry professionals. This article presents a case study of implementing an information security management system at one enterprise, part of the Belenergo State Production Association of the Ministry of Energy of the Republic of Belarus, and an interpretation of the results.

Keywords: energy; information security; information protection; management systems; standards; certification; cybersecurity; information security risks; 27001.

Введение

Энергетика по праву относится к системообразующим компонентам национальной экономики и постоянно подвержена всем протекающим в ней процессам, в том числе цифровизации. Уязвимой точкой последней является восприимчивость к кибератакам, что ставит актуальную задачу по эффективному управлению процессами информационной безопасности (ИБ) в производственной деятельности организаций и предприятий.

Проблематика ИБ на объектах энергетики исследовалась белорусскими и российскими авторами С. Ю. Воробьевым, А. И. Белоусом, И. Н. Колоском [1–3]. Эффективность внедрения системы менеджмента ИБ (далее – СМИБ) в операционную деятельность организаций анализировалась в работах А. А. Кайсаровой, А. Т. Касымбека П. А. Лончих [4–6].

Вместе с тем в настоящее время отсутствуют исследования, посвященные изучению эффективности от внедрения СМИБ в производственную деятельность организаций и предприятий энергетической отрасли. Целью работы является рассмотрение практического кейса по внедрению СМИБ в деятельность одного из предприятий, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее – Предприятие), интерпретация полученных от его реализации результатов, возможность их имплементации в производственную деятельность белорусских энергетических организаций и предприятий.

Основная часть

Серия стандартов ISO/IEC 270xx, принятая Международной организацией по стандартизации ISO (International Organization for Standardization), представляет собой набор общепризнанных лучших практик и требований, предъявляемых к СМИБ. После осуществления перевода и терминологической адаптации Государственным комитетом по стандартизации Республики Беларусь данные технические нормативные правовые акты) были введены в действие на территории Республики Беларусь (по содержанию и смысловой нагрузке они полностью идентичны стандартам ISO).

Организации белорусской энергетической системы вынуждены проводить комплекс мероприятий организационного, правового и технического характера для защиты самого ценного информационного общества: информации. Одним из направлений повышения состояния защищенности информационных активов является разработка и внедрение СМИБ в соответствии с требованиями СТБ 27001, общепринятого набора мировых лучших практик в сфере защиты информации. Интеграция СМИБ в практическую деятельность любой организации вне зависимости от рода деятельности, принадлежности к государственному или частному сектору, численности позволяет вовлечь высший менеджмент в непосредственное участие управления процессами ИБ, идентифицировать и минимизировать риски ИБ, продемонстрировать контрагентам, органам государственного управления, контрольным и надзорным инстанциям приверженность выполнения нормативных требований ИБ, четко разделить обязанности и полномочия в сфере защиты информации, привить собственным работникам культуру защиты информации, укрепить деловую репутацию, и, соответственно, увеличить собственные доходы и инвестиционную привлекательность.

Подтверждение соответствия СМИБ требованиям СТБ 27001, подтвержденное сертификатом в Национальной системе подтверждения соответствия, ставит перед Предприятием очередную амбициозную задачу: осуществление мероприятий на получение лицензии по проектированию, созданию и аудиту систем информационной безопасности критически важных объектов информатизации.

Заключение

СМИБ не является панацеей от хищения конфиденциальной информации, коммерческого шпионажа, или кибератак на АЭС, но проведение мероприятий согласно методологии, основанной на рискориентированном подходе, описанной в СТБ 27001 позволит повысить защищенность самого ценного ресурса XXI века: информации.

Список использованных источников

1. Воробьев, С. Ю. Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности / С. Ю. Воробьев, Е. А. Ханчевский // Энергетическая стратегия. – 2024. – Т. 102, № 6. – С. 33–36.
2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А.И. Белоус. – Москва ; Вологда : Инфра-Инженерия, 2020. – 644 с.
3. Анализ кибербезопасности объектов энергетики с учетом механизма и кинетики нежелательных процессов / И. Н. Колосок, Е. С. Коркина // Энергетик. – 2024. – № 2. – С. 3–8.

4. Внедрение международного стандарта ИСО/МЭК 27001 – основа управления информационной безопасностью предприятия / А. А. Кайсарова, А. К. Тулекбаева, А. А. Токтабек [и др.] // Вестник науки Южного Казахстана. – 2018. – № 4 (4). – С. 103–106.

5. Касымбек, А. Т. Польза от внедрения международного стандарта ISO/IEC 27001 / А. Т. Касымбек // Евразийское Научное Объединение. – 2015. – Т. 1, № 2(2). – С. 52–53.

6. Лончих, П. А. Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии / П. А. Лончих, О. М. Сафонова // Системы. Методы. Технологии. – 2020. – № 4(48). – С. 80–87.

References

1. Vorobyov, S. Yu. Cyberattacks on Critical Energy Facilities as a Source of National Security Threats / S. Yu. Vorobyov, E. A. Khanchevsky // Energy Strategy. – 2024. – Vol. 102, No. 6. – P. 33–36.

2. Belous, A. I. Cybersecurity of Fuel and Energy Complex Facilities. Concepts, Methods, and Means of Support / A. I. Belous. – Moscow; Vologda: Infra-Engineering, 2020. – 644 p.

3. Analysis of Cybersecurity of Energy Facilities Taking into Account the Mechanism and Kinetics of Undesirable Processes / I. N. Kolosok, E. S. Korkina // Energetik. – 2024. – No. 2. – P. 3–8.

4. Implementation of the international standard ISO / IEC 27001 – the basis for enterprise information security management / A. A. Kaisarova, A. K. Tulekbaeva, A. A. Toktabek [et al.] // Bulletin of Science of South Kazakhstan. – 2018. – No. 4 (4). – P. 103–106.

5. Kasymbek, A. T. Benefits of implementing the international standard ISO / IEC 27001 / A. T. Kasymbek // Eurasian Scientific Association. – 2015. – Vol. 1, No. 2 (2). – P. 52–53.

6. Lontsikh, P. A. Methodology for the creation and implementation of an information security management system at an industrial enterprise / P. A. Lontsikh, O. M. Safonova // Systems. Methods. Technologies. – 2020. – No. 4 (48). – P. 80–87.

Сведения об авторах

Воробьёв С.Ю., магистр технических наук, заведующий сектором информационной безопасности отдела информационных технологий организации научно-исследовательского и проектно-изыскательского республиканского унитарного предприятия «Белэнергосетьпроект», s.varabyou@besp.by.

Ханчевский Е.А., начальник отдела информационных технологий организации научно-исследовательского и проектно-изыскательского республиканского унитарного предприятия «Белэнергосетьпроект», zh@besp.by.

Information about the authors

Vorobyov S.Yu., Master of Engineering Sciences, Head of the Information Security Sector, Information Technology Department, Research and Design and Survey Organization, Republican Unitary Enterprise «Belenergosetproekt», s.varabyou@besp.by.

Khanchevsky E.A., Head of the Information Technology Department, Research and Design and Survey Organization, Republican Unitary Enterprise «Belenergosetproekt», zh@besp.by.

УДК 004.056

ПРИМЕНЕНИЕ ОБУЧАЮЩИХ ИГР ДЛЯ ФОРМИРОВАНИЯ СПЕЦИАЛЬНЫХ НАВЫКОВ ПО ЗАЩИТЕ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Я.А. Клиндухов¹, С.Д. Мажаева¹, О.В. Бойправ²,

¹*Учреждение образования «Национальный
детский технопарк», г. Минск, Беларусь*

²*Учреждение образования «Белорусский государственный
университет информатики и радиоэлектроники», г. Минск, Беларусь*

Аннотация. В данной работе рассматривается проблема роста угроз информационной безопасности в условиях стремительной цифровизации всех сфер жизни Республики Беларусь. Обосновано применение образовательных игр как эффективного инструмента для формирования специальных навыков по защите от угроз информационной безопасности и преодоления разрыва между техническими возможностями программных средств и реальными навыками пользователей. Описана разработка обучающей игры на языке Python и фреймворке Pygame, представляющей собой симулятор практических задач специалиста отдела информационной безопасности организации. Обучающей игрой моделируются угрозы информационной безопасности согласно этапам модели Cyber Kill Chain. Приведены результаты апробации среди учащихся Национального детского технопарка, подтверждающие высокую эффективность обучения: прирост среднего арифметического отметок после прохождения игры составил более 20 %. Доказана эффективность обучающих игр в системе подготовки специалистов по информационной безопасности.

Ключевые слова: обучающие игры, цифровизация, угрозы информационной безопасности, человеческий фактор, средства защиты информации, моделирование угроз информационной безопасности, методика обучения, эффективность обучающей игры, апробация обучающей игры, подготовка специалистов по информационной безопасности.

APPLICATION OF EDUCATIONAL GAMES FOR THE FORMATION OF SPECIAL SKILLS IN PROTECTION AGAINST INFORMATION SECURITY THREATS

Y.A. Klindukhov¹, S.D. Mazhaeva¹, O.V. Boiprav²

²*Educational Institution "National Children's Technopark",
Minsk, Republic of Belarus*

¹*Educational Institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. This paper examines the problem of the growth of information security threats in the context of the rapid digitalization of all spheres of life in the Republic of Belarus. The use of educational games as an effective tool for the formation of basic skills to protect against information security threats and to bridge the gap between the technical capabilities of software and the real skills of users is substantiated. The development of an educational game in Python and the Pygame framework is described, which is a simulator of practical tasks of a specialist in the information security department of an organization.

The educational game simulates information security threats according to the stages of the Cyber Kill Chain model. The results of the testing among students of the National Children's Technopark are presented, confirming the high effectiveness of training: the increase in the arithmetic mean of the marks after passing the game was more than 20 %. The effectiveness of educational games in the training of information security specialists has been proven.

Keywords: educational games, digitalization, information security threats, human factor, information security tools, information security threat modeling, teaching methodology, educational game effectiveness, educational game testing, information security specialist training.

Введение

В условиях стремительной цифровизации всех сфер жизни Республики Беларусь наблюдается значительный рост угроз информационной безопасности [1–3]. Несмотря на наличие современных технических средств защиты информации, ключевой проблемой остается человеческий фактор. Согласно исследованиям Ponemon Institute, 75 % инцидентов в более чем 310 компаниях по всему миру связаны именно с ошибками пользователей информационных систем.

В таких условиях появляется значительный разрыв между техническими возможностями программных средств защиты информации и реальными навыками пользователей по их применению. В связи с этим одной из наиболее важных задач является внедрение новых образовательных подходов, среди которых особое место занимают образовательные игры, для подготовки специалистов в области защиты информации.

Основная часть

Под образовательными играми будем понимать игры, которые разработаны специально для обучения определенным предметам или навыкам [4]. Отличие образовательной игры от компьютерной заключается в получении обучающимися новых специальных знаний, наличии четкой учебной цели и педагогического результата, в то время как компьютерная игра фокусируется на развлечении, хотя и может иметь побочный образовательный эффект.

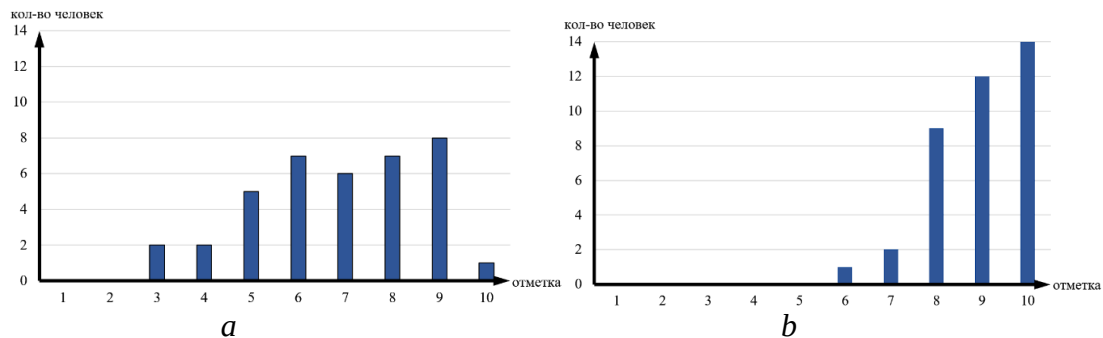
Также, обучающие игры имеют эффективное применение в области информационной безопасности, так как они позволяют моделировать реальные угрозы информационной безопасности, формируя необходимые практические и теоретические навыки. Большинство таких игр носят симуляционный характер, моделируя обучающемуся ситуацию, похожую на реальную. Особенностью таких симуляторов является возможность генерации конкретных угроз информационной безопасности, таких как внедрение вредоносного кода в процессы, использование легитимных

учетных записей, почтовый фишинг и другие. Такой подход обеспечивает высокую заинтересованность обучающегося в процессе, позволяя добиться высокой эффективности обучения в короткие сроки. Кроме того, специалистам по защите информации часто требуется поиск неординарных решений, а игровые технологии способствуют развитию творческого потенциала и стратегического мышления, необходимого для решения задач проектирования и защиты информационных систем.

Для оценки эффективности образовательных игр в области информационной безопасности в рамках данной работы разработана обучающая игра, направленная на выбор средств защиты от угроз информационной безопасности. Для реализации игры использовался язык программирования Python 3.14.0 и фреймворк Pygame 2.5.0, что позволило создать игровой проект, не требующий больших вычислительных ресурсов. Жанр игры определен как симулятор практических задач специалиста отдела информационной безопасности организации.

Сюжет игры следующий. Игрок выступает в роли нового сотрудника отдела информационной безопасности вымышленной компании «ТехноПро». Действие разворачивается внутри интерфейса персонального компьютера сотрудника, состоящего из различных программ, с которыми игроку предстоит взаимодействовать (SIEM–система, антивирусная программа, система анализа трафика и другие). Далее в игре моделируется угроза информационной безопасности, которую игрок должен выявить, идентифицировать, проанализировать и устранить. Важно отметить, что деятельность нарушителя в игре представлена в виде последовательных этапов, согласно этапам модели нарушителя Cyber Kill Chain [5].

Для количественной оценки эффективности разработанной обучающей игры было предложено собрать первичные знания по теме угроз информационной безопасности, которые реализованы в игре, в виде тестирования с выбором из 4 вариантов ответов. Всего вопросов 10, поэтому оценка осуществлялась по 10-балльной системе. Далее было предложено полностью пройти игру. После прохождения игры было предложено снова пройти те же 10 вопросов для выявления вторичных знаний. Результаты тестирования до прохождения игры представлены на части *а* рисунка, а результаты после тестирования – на части *б* рисунка. Выборка составила 38 человек, учащихся Национального детского технопарка образовательных направлений (лазерные технологии, электроника и связь, информационные и компьютерные технологии, инженерная экология и другие).



Распределение отметок до прохождения обучающей игры (a) и после (b)
Distribution of marks before completing the educational game (a) and after (b)

Как видно из результатов, до тестирования средний балл составил 6.87 балла, а после игры данное значение составило 8.95 балла. Прирост среднего балла до и после игры составил 2.08 балла, что говорит о приросте значений более чем в 20%. Данные результаты свидетельствуют о высокой эффективности обучающей игры. Также отзывы участников исследования говорят о высоком уровне заинтересованности обучающей игрой, что выделяет игру среди других видов обучающих материалов.

Заключение

В ходе исследования было обосновано применение обучающей игры как эффективного инструмента для формирования специальных навыков по защите от угроз информационной безопасности. Разработанный симулятор практических задач специалиста отдела информационной безопасности позволил реализовать интерактивный подход к обучению. Моделирование реальных сценариев атак (в соответствии с моделью Cyber Kill Chain) в безопасной среде дало возможность обучающимся не только ознакомиться с интерфейсом программного обеспечения, но и выявить, идентифицировать, проанализировать и устранить угрозы информационной безопасности.

Результаты экспериментальной апробации, проведенной среди учащихся Национального детского технопарка, подтвердили высокую эффективность разработанной обучающей игры. Сравнительный анализ данных первичного и вторичного контроля показал прирост среднего балла успеваемости с 6.87 до 8.95, что составляет более 20%.

Таким образом, обучающие игры могут быть эффективным средством для подготовки специалистов в области защиты информации. Использование образовательных игр способствует повышению уровня знаний в области информационной безопасности. Помимо улучшения количественных показателей успеваемости, данный подход обеспечивает высокую вовлеченность обучающихся, развивает аналитическое и стратегическое мышление, что делает внедрение обучающих

перспективным направлением в системе подготовки специалистов по информационной безопасности.

Список использованных источников

1. Барило К. С., Нестеренков С. Н., Бегляк Е. В. (2025) Криптографические методы защиты информации в сфере электронного документооборота. *Технические средства защиты информации*. 66–69.
2. Мырадов П. С., Мырадов П. С. (2025) Технические средства защиты информации: современные технологии, методы и перспективы. *Технические средства защиты информации*. 260–263.
3. Дроздов М. М., Прудник А. М. (2017) Анализ состояния и методология обеспечения безопасности информационных систем. *Технические средства защиты информации*. 15–16.
4. Рябинин Н. С. (2025) Многофункциональный веб-сервис для тестирования и интерактивных игр с использованием искусственного интеллекта. *Радиотехника и электроника*. 171–175.
5. Борботько Т. В., Бойправ О. В., Тимофеев А. М. (2025) *Основы информационной безопасности*. Минск, Издательство «БГУИР»

References

1. Barilo K. S., Nesterenkov S. N., Beglyak E. V. (2025) Cryptographic Methods of Information Protection in the Field of Electronic Document Management. *Technical Information Security Tools*. 66–69 (in Russian).
2. Myradov P. S., Myradov P. S. (2025) Technical Information Security Tools: Modern Technologies, Methods and Prospects. *Technical Information Security Tools*. 260–263 (in Russian).
3. Drozdov M. M., Prudnik A. M. (2017) State Analysis and Methodology for Ensuring the Security of Information Systems. *Technical Information Security Tools*. 15–16 (in Russian).
4. Ryabinin N. S. (2025) Multifunctional Web Service for Testing and Interactive Games Using Artificial Intelligence. *Radio Engineering and Electronics*. 171–175 (in Russian).
5. Borbotko T. V., Boiprav O. V., Timofeev A. M. (2025) *Fundamentals of Information Security*. Minsk, BSUIR Publishing House (in Russian).

Сведения об авторах

Клиндухов Я.А., учащийся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», klinduhov.science@gmail.com.

Мажаева С.Д., учащаяся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», sd.mazhaeva2009@gmail.com.

Бойправ О.В., канд. техн. наук, доц., зав. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», smu@bsuir.by.

Information about the authors

Klindukhov Y.A., Student of the direction “Information Security”, Educational Institution “National Children's Technopark”, klinduhov.science@gmail.com.

Mazhaeva S.D., Student of the direction “Information Security”, Educational Institution “National Children's Technopark”, sd.mazhaeva2009@gmail.com.

Boiprav O.V., Cand. Sci. (Tech.), Associate Professor, Head of the Information Protection Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, smu@bsuir.by.

УДК 330.336

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПОДГОТОВКЕ КАДРОВ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ

А.М. Воронина

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Одновременно с развитием цифровой экономики возрастает и число угроз информационной безопасности, что актуализирует подготовку специалистов с соответствующими компетенциями. В данной работе рассматриваются теоретические основы формирования компетенций при подготовке кадров в области защиты информации, существующие образовательные программы в Республике Беларусь, а также анализируются проблемы цифровой трансформации экономики, включая защиту критической инфраструктуры, персональных данных и противодействие кибермошенничеству. Помимо этого, сформированы предложения по усовершенствованию обучения специалистов.

Ключевые слова: информационная безопасность; защита информации; профессиональные навыки; компетенции; подготовка кадров; международные стандарты; цифровая экономика; кадровый потенциал; устойчивое развитие; цифровая трансформация.

FORMATION OF INFORMATION PROTECTION COMPETENCIES IN THE TRAINING OF PERSONNEL FOR THE DIGITAL ECONOMY OF THE REPUBLIC OF BELARUS

A.M. Voronina

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. As the digital economy develops, the number of information security threats increases, making it necessary to train specialists with relevant competencies. This paper examines the theoretical foundations of competency development in information security training, existing educational programs in the Republic of Belarus, and analyzes the challenges of digital transformation in the economy, including the protection of critical infrastructure, personal data, and countering cyber fraud. Additionally, the paper provides suggestions for improving the training of specialists.

Keywords: information security; information protection; professional skills; competencies; personnel training; international standards; digital economy; human resources; sustainable development; digital transformation.

Введение

Цифровизация экономики является одним из национальных приоритетов Республики Беларусь, так как она не только охватывает все сферы, но и способствует повышению конкурентоспособности экономики. Тем не менее с ростом цифровой трансформации появляются и новые риски и угрозы информационной безопасности, что делает защиту информации критически важным фактором устойчивого развития и национальной безопасности государства.

Следовательно, возрастает потребность в подготовке квалифицированных кадров, обладающих актуальными компетенциями в сфере информационной безопасности. Таким образом адаптация системы образования к актуальным вызовам и национальным становится стратегической задачей государства.

Цель статьи – рассмотреть теоретические основы формирования компетенций при подготовке кадров в области защиты информации, проанализировать проблемы цифровой экономики, а также дать предложения по усовершенствованию обучения специалистов.

Основная часть

Понятие «компетенция» подразумевает процесс применения знаний, навыков, умений, а также личностных качеств и профессионального опыта к конкретным задачам определенной области. Что касается защиты информации, основой для образовательных программ и формирования требований к подготовке специалистов являются международные стандарты (ISO/IEC 27001, NIST Cybersecurity Framework) и нормативные правовые документы Республики Беларусь [1].

Подготовка кадров в области защиты информации осуществляется на базе ведущих университетов (БГУИР, БГУ, АУППРБ), профильных факультетов, а также колледжей и техникумов. Ключевыми являются дисциплины, связанные с управлением информационной безопасностью, криптографией, защитой информационных сетей и правовыми аспектами информационной безопасности. Кроме того, образовательные программы подразумевают также наличие специализированных лабораторий и участие обучаемых в научных конференциях, конкурсах и проектах, что способствует формированию практико-ориентированных компетенций.

Эффективность приобретенных компетенций определяется успешным результатом их применения в условиях современных вызовов экономики. С высоким темпом цифровизации, что обуславливает увеличение объема данных, защита критической инфраструктуры и персональных данных,

а также борьба с кибермошенничеством становятся особо значимыми в рамках государства. Недостаток компетентных специалистов в данной области может привести к значительным убыткам, рискам для бизнеса и угрозам национальной безопасности. На сегодняшний день проблема преодоления компетентностных разрывов в условиях цифровизации экономики является крайне актуальной [2].

Для обеспечения устойчивого развития и высокого уровня защиты информации необходимо повысить качество подготовки кадров. В виде решения можно рассматривать внедрение в программы модулей с реальными кейсами белорусских организаций, а также увеличение количества специализированных лабораторий для практических занятий при содействии государственных структур и ИТ-компаний. Помимо этого, немаловажным является и повышение квалификации преподавателей, так как подготовка кадров напрямую зависит от их уровня профессионализма. Повышение квалификации может включать в себя не только курсы и тренинги, но и обмен знаниями и опытом с зарубежными представителями сферы информационной безопасности.

Заключение

Таким образом, формирование компетенций при подготовке кадров в области защиты информации становится одним из ключевых факторов эффективной цифровизации экономики Республики Беларусь. Проблемы, относящиеся к цифровизации, требуют регулярного совершенствования образовательных программ. Внедрение предложенных решений позволит не только обеспечить устойчивое цифровое развитие государства, но и значительно повысит уровень информационной безопасности.

Список использованных источников

1. Вострецова Е. В. Основы информационной безопасности : учебное пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с.
2. Ворожцова А. В., Гончарова Н. В. Развитие цифровых компетенций персонала как средство повышения информационной безопасности организации // XVII международная конференция «Российские регионы в фокусе перемен» : сборник докладов (Екатеринбург, 17–19 ноября 2022 г.). Екатеринбург : ООО Издательский Дом «Ажур», 2023. С. 260-264.

References

1. Vostretsova E. V. (2019) Fundamentals of Information Security. Yekaterinburg, Ural University Press. (In Russian).
2. Vorozhtsova A. V., Goncharova N. V. (2023) Development of Digital Competencies of Personnel as a Means of Improving the Information Security of an Organization. XVII International Conference “Russian Regions in the Focus of Changes” : Collection of Reports. Yekaterinburg, Azhur Publishing House, pp. 260-264. (In Russian).

Сведения об авторе

Воронина А.М., ассистент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.voronina@bsuir.by.

Information about the author

Voronina A.M., assistant, Educational Establishment “Belarusian State University of Informatics and Radioelectronics”, a.voronina@bsuir.by.

УДК 621.794.61

МОДЕЛИРОВАНИЕ ВЫХОДНЫХ ХАРАКТЕРИСТИК ПОЛЕВЫХ ТРАНЗИСТОРОВ С ИСПОЛЬЗОВАНИЕМ ГРАФЕНА И ЕГО МОДИФИКАЦИЙ В ДИАПАЗОНАХ СВЧ И КВЧ

В.Н. Мищенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Графен, обладающий высокой подвижностью заряда, которая превышает подвижность носителей заряда для всех известных материалов, рассматривается в настоящее время как один из наиболее перспективных материалов для создания новых полупроводниковых приборов. Приведены результаты моделирования выходных характеристик полевых транзисторов с использованием графена и его модификаций в диапазонах СВЧ и КВЧ. Моделирование выполнялось с использованием метода Монте Карло, который позволяет исследовать основные выходные характеристики полевых транзисторов, содержащих области графена и модифицированного графена. Полученные в результате моделирования характеристики и параметры полевых транзисторов могут быть использованы для создания новых устройств диапазонов СВЧ и КВЧ, обладающих улучшенными выходными параметрами и характеристиками.

Ключевые слова: графен; фтор; водород; моделирование; полевой транзистор.

MODELING OF OUTPUT CHARACTERISTICS OF FIELD-EFFECT TRANSISTORS USING GRAPHENE AND ITS MODIFICATIONS IN THE MICROWAVE AND MWR RANGE

V.N. Mishchanka

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. Graphene, which possesses high charge carrier mobility and velocity, exceeding that of all known materials, is currently considered one of the most promising materials for the creation of new semiconductor devices. The results of modeling the output characteristics of field-effect transistors using graphene and its modifications in the microwave and millimeter-wave ranges are presented. The modeling was performed using the Monte Carlo method, which allows one to investigate the key output characteristics of field-effect transistors containing graphene and modified graphene regions. The characteristics and parameters of the field-effect transistors obtained from the modeling can be used to create new microwave and millimeter-wave devices with improved output parameters and characteristics.

Keywords: graphene; fluorine; hydrogen; modeling; field-effect transistor.

Введение

Исследования, выполненные в последние годы, показали, что графен, представляющий собой двухмерный слой углерода, обладает совокупностью ряда уникальных свойств и характеристик, например, большой механической жесткостью и рекордно большой теплопроводностью. Но одно из свойств графена – высокая подвижность носителей заряда, которая является одной из самой высокой среди всех известных материалов, делает его перспективным материалом для использования в электронике и прогнозирует в будущем возможную замену более изученных и популярных материалов в интегральных микросхемах [1]. Однако для реализации уникальных свойств графена необходима разработка и исследование новых полевых транзисторов диапазонов СВЧ и КВЧ на основе графена и его модификаций с использованием атомов водорода, фтора и других элементов.

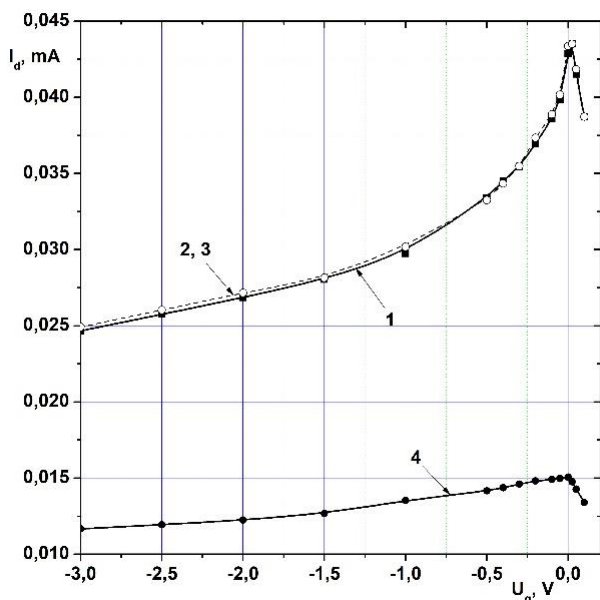
Метод и особенности моделирования характеристик графена и его модификаций, входящих в состав полевых транзисторов

Моделирование из первых принципов графена и его модификаций, входящих в состав полевых транзисторов, было выполнено с помощью программных комплексов Quantum Espresso [2] и EPW [3]. Использовалось обобщенное градиентное приближение вида GGA при параметризации Perdew-Burke-Ernzerhof (PBE). Были применены следующие параметры моделирования: энергия отсечки волновой функции составляла величину 60 Ry ($1 \text{ Ry} \approx 13,605 \text{ эВ}$), энергия отсечки плотности заряда и потенциалов – 350 Ry, зона Бриллюэна была представлена с помощью сетки Монкхорста-Пака размером $12 \times 12 \times 1$. С помощью программного комплекса EPW были получены зависимости интенсивностей рассеивания носителей заряда для графена и его модификаций с использованием атомов водорода и фтора – C_2H_2 или C_2F_2 [4], которые далее были использованы в программе моделирования выходных характеристик исследованного полевого транзистора.

Для анализа полевого транзистора, который включал в себя области графена и его модификаций с использованием атомов водорода или фтора, была разработана программа, в которой использовался метод Монте-Карло. Рассматривались следующие основные механизмы рассеивания носителей заряда в графене и его модификациях с использованием атомов водорода и фтора: на оптических фононах, на примесях, на акустических фононах. Путем моделирования получены основные выходные характеристики – зависимости выходного тока стока от величины постоянного напряжения на затворе, которые позволили получить зависимости коэффициента усиления исследуемого полевого транзистора. Моделирование выполнялось для значения температуры

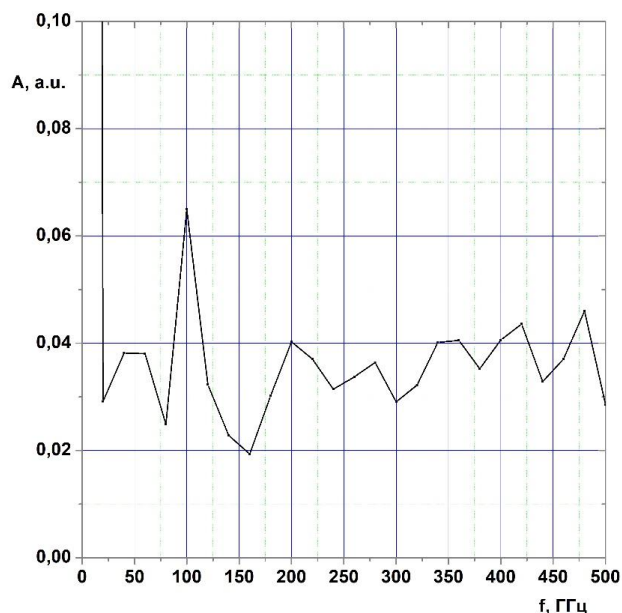
$T = 300$ К, концентрации электронов в слоях графена, гидрированного графена и GaAs равном $1 \cdot 10^{16} \text{ см}^{-3}$. Общая длина структуры принималась равной $1 \cdot 10^{-6}$ м, длина затвора – равной $0,2 \cdot 10^{-6}$ м. Кривая 1 на рисунке а получена для конструкции при использовании только слоя графена на подложке из арсенида галлия без областей гидрированного или фторированного графена. Кривые 2 и 3 на рис. а получены для конструкции, которая содержит области графена и область модификации графена с использованием атомов водорода или фтора. Кривая 4 на рисунке а получена для конструкции при использовании только материала арсенид галлий, т.е. без использования слоев графена и областей гидрированного или фторированного графена. Анализ кривых 1–4, представленных на рисунке а, показывает, что выходной ток полевого транзистора, который содержит области графена и его модификации с использованием атомов водорода и фтора, имеет большую величину по сравнению с конструкцией, которая не имеет графена и гидрированного или фторированного графена.

Для представленной структуры путем моделирования была получена зависимость выходного тока полевого транзистора со слоем графена и гидрированного графена при подаче на вход, т.е. к ее затвору, внешнего гармонического сигнала с частотой 100 ГГц и амплитудой $U_s = 0,003$ В в диапазоне КВЧ.



а. Зависимости выходного тока стока от величины напряжения на затворе

a. Dependence of the output drain current on the gate voltage



б. Спектральная характеристика выходного сигнала полевого транзистора с использованием

графена и гидрированного графена
b. Spectral characteristic of the output signal of a field-effect transistor using graphene and hydrogenated graphene

На рис. б показана действительная часть комплексной амплитуды спектра, которая была получена путем преобразования Фурье, которое было применено к массиву полученных данных зависимости выходного тока от времени. Таким образом, за счет использования графена и его модификации – гидрированного и фторированного графена может быть получена возможность улучшения выходных характеристик в диапазоне КВЧ по сравнению с известными полевыми транзисторами, разработанными без использования графена и его модификаций.

Заключение

Установлено, что применение графена и его модификаций с использованием атомов водорода или фтора позволяет получить более высокие значения выходного тока полевого транзистора (приблизительно, на 30–50 %), высокие значения крутизны выходной характеристики и коэффициента усиления в сравнении со аналогичными полевыми транзисторами, которая не используют графен и его модификации. Эти обстоятельства, учитывая высокую подвижность и скорость носителей заряда в слое графена, должны обеспечить хорошие выходные характеристики и широкий частотный диапазон работы разрабатываемых с использованием графена и его модификаций новых функциональных приборов и устройств диапазонов СВЧ и КВЧ.

Список использованных источников / References

1. Novoselov K. S., Geim A. K., et al. (2004) Electric field effect in atomically thin carbon film. *Science*, 306, 666-669.
2. Giannozzi P., Baroni S., Bonini N., Calandra M., Car R., Cavazzoni C., et al. (2009) QUANTUM ESPRESSO: a modular and open-source software project for quantum simulations of materials. *J. Phys.: Condens. Matter*. 21. 395502.
3. Lee H., Poncé S., Bushick K., Hajinazar S., Lafuente-Bartolome J., Leveillee J., et al. (2023) Electron-phonon physics from first principles using the EPW code. *npj Computational Materials*. 9. 156.
4. Mishchanka V.N. (2024) First-principles modeling of electron-phonon scattering rates in graphene. *Modern Electronic Materials*. 10 (3). 177-184.

Сведения об авторе

Мищенко В.Н., канд. техн. наук, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, mishchenko@bsuir.by

Information about the author

Mishchanka V.N., PhD, associate professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus, mishchenko@bsuir.by.

УДК 377.031

АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.Г. Ручаевская, В.В. Шаталова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь

Аннотация. Обеспечение информационной безопасности сегодня очень актуально. Информационную безопасность можно выделить как одну из основных информационных проблем XXI века. На самом деле, проблемы хищения информации, искажения смысла информации и ее уничтожения часто приводят к последствиям, ведущим не только к банкротствам фирм, но и возможным жертвам.

Ключевые слова: информационная безопасность; несанкционированный доступ; субъекты информационных отношений; информационные системы.

ASPECTS OF INFORMATION SYSTEMS SECURITY ENSURING

E.G. Ruchaevskaya, V.V. Shatalova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", Minsk, Republic of Belarus

Abstract. Ensuring information security is highly relevant today. Information security can be identified as one of the key information challenges of the 21st century. Indeed, information theft, distortion, and destruction often lead to consequences that not only lead to company bankruptcies but also to potential casualties (not to mention military conflicts).

Keywords: information security; unauthorized access; subjects of information relations; information systems.

Введение

Безопасность информационной системы можно определить, как ее состояние, при котором обрабатываемая в ней информация характеризуется конфиденциальностью, целостностью и доступностью [1]. Для достижения указанного состояния необходимо реализовать комплекс мер по защите информации, обрабатываемой в информационной системе. Рассмотрим ключевые аспекты обеспечения безопасности информационных систем.

Основная часть

Меры по защите информации, обрабатываемой в информационной системе, должны быть направлены на:

- выявление критической информации;
- физическую защиту оборудования информационной системы;
- защита критической информации от несанкционированного доступа;
- обеспечение целостности критической информации и связанных с ней процессов (создания, ввода, обработки и вывода);
- обеспечение доступности информации;
- учет всех процессов, связанных с информацией [2].

Основные аспекты защиты информации от несанкционированного доступа:

- присвоение пользователю, файлам, компьютерным программам и каналам связи идентификаторов – уникальных имен и кодов;
- установление подлинности при обращениях к информационной системе и информации, по сути, проверка соответствия лица или устройства, сообщившего идентификатор (такая идентификация пользователей, программ, терминалов при доступе к системе зачастую выполняется посредством проверки паролей или обращением в службу, которая отвечает за сертификацию пользователей).

Основные аспекты обеспечения целостности и доступности информации следующие:

- защита процессов создания информации, ее ввода, обработки и вывода;
- учет всех событий, связанных с управлением информацией (когда информация создается, модифицируется, когда к ней обеспечивается доступ и когда она распространяется).

Заключение

В заключении можно отметить, что правильный с методологической точки зрения подход к обеспечению безопасности информационных систем начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием указанных систем.

Список использованных источников

1. Абразовский Ю.Д., Ручаевская Е.Г. (2024) Безопасность информационных технологий. 60-ая научно-практическая конференция аспирантов, магистрантов и студентов БГУИР. Научная конференция учащихся филиала БГУИР «Минский радиотехнический колледж», 17–18.
2. Ручаевская Е.Г., Шаталова В.В. (2025) Защита информации в информационно-вычислительных системах. Технические средства защиты информации : материалы

XXIII Международной научно-технической конференции. (Республика Беларусь, Минск, 08 апреля 2025 года) / редкол. : О. В. Бойправ [и др.]. – Минск : БГУИР, 2025.

References

1. Abrazovsky Yu.D., Ruchaevskaya E.G. (2024) Information Technology Security. 60th Scientific and Practical Conference of Postgraduate, Master's, and Undergraduate Students of BSUIR. Scientific Conference of Students of the BSUIR Branch "Minsk Radio Engineering College", 17-18.
2. Ruchaevskaya E.G., Shatalova V.V. (2025) Information Security in Information Systems. Technical Means of Information Security: Proceedings of the XXIII International Scientific and Technical Conference. (Republic of Belarus, Minsk, April 8, 2025) / ed. board: O. V. Boiprav [et al.]. - Minsk: BSUIR, 2025.

Сведения об авторах

Ручаевская Е.Г., канд. пед. наук, доц., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», elenruch@gmail.com.

Шаталова В.В., канд. техн. наук, доц., директор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», филиал «Минский радиотехнический колледж», shatalova@bsuir.by

Information about the authors

Ruchaevskaya E.G., Cand. Sci. Ped., Associate Professor, teacher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", elenruch@gmail.com.

Shatalova V.V., Cand. Sci. Tech., Associate Professor, director, Educational Institution "Belarusian State University of Informatics and Radioelectronics", branch "Minsk Radio Engineering College", shatalova@bsuir.by.

УДК 004.56+003.26

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОСУЩЕСТВЛЕНИЯ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ МОДИФИКАЦИИ ПОЛУТОНОВЫХ ОТТЕНКОВ РАСТРИРОВАННЫХ ДОКУМЕНТОВ

М.Г. Савельева

Учреждение образования «Белорусский государственный технологический университет», г. Минск, Республика Беларусь

Аннотация. Доклад описывает разработанное приложение, предназначенное для стеганографических преобразований растрированных текстовых документов-контейнеров. Основными функциями выступают внедрение и извлечение сообщения. Ключевой особенностью разработанного программного средства инструмента является интеграция модуля для всестороннего статистического анализа выполненных операций. Данный модуль позволит пользователям отслеживать и визуализировать

метрики, связанные со стеганографией, такие как частота использования ключей, распределение длин сообщений и эффективность операций.

Ключевые слова: стеганография, стеганографический анализ, растривание, полутонные оттенки, программные средства, Python, Kivy, Mathplotlib, Pillow, Numpy.

A SOFTWARE TOOL FOR PERFORMING STEGANOGRAPHIC TRANSFORMATION BASED ON MODIFICATION OF HALFTONE SHADES OF RASTERIZED DOCUMENTS

M.G. Saveleva

*Educational Institution “Belarusian State Technological University”,
Minsk, Republic of Belarus*

Abstract. The report describes a developed application designed for steganographic transformations of rasterized text container documents. The main functions are message embedding and extraction. The key feature of the developed software of the tool is the integration of a module for a comprehensive statistical analysis of the performed operations. This module will allow users to track and visualize metrics related to steganography, such as key usage frequency, message length distribution, and operational efficiency.

Keywords: steganography, steganographic analysis, rasterization, halftone shades, software, Python, Kivy, Mathplotlib, Pillow, Numpy.

Введение

Несмотря на наличие разнообразных решений, реализующих основные функции скрытия данных, практически все они лишены встроенных средств для сбора и анализа статистики использования. Это позволило четко сформулировать основную цель и уникальность разрабатываемого программного средства: создание стеганографического инструмента, который позволяет объединять функции преобразования документа-контейнера с возможностями статистического анализа и визуализации.

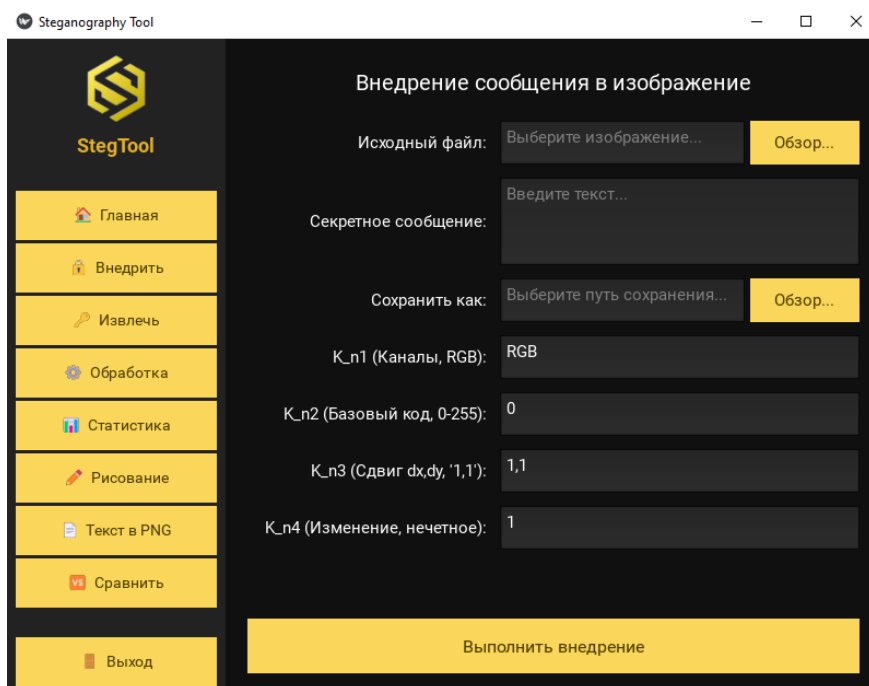
Основная часть

Ранее была предложена модель и, синтезированная на ее основе, структурная схема стеганографической системы, основанные на модификации пространственной области и цветовых параметров пикселей растриванного документа-контейнера [1]. Для реализации описанных стеганографических методов (внедрение/извлечение сообщение и статистическая обработка стегоконтейнера) разработано специализированное приложение (рабочее название – StegTool) на основе языка программирования Python.

Выбор языка обусловлен его обширной стандартной библиотекой и многочисленной экосистемой сторонних пакетов. Для создания кроссплатформенного графического пользовательского интерфейса был задействован фреймворк Kivy, позволяющий создавать единую кодовую базу для Windows, Linux и macOS. Для низкоуровневых манипуляций

с изображениями, включая чтение, запись и пиксельное редактирование, была использована библиотека Pillow, являющаяся стандартом в экосистеме Python. Визуализация статистических данных была реализована с помощью библиотеки Matplotlib, предоставляющей широкие возможности для построения научных графиков и гистограмм.

Была спроектирована общая структура пользовательского интерфейса, в центре которой лежит принцип обеспечения интуитивно понятного взаимодействия. Разработана единая дизайн-система, включающая боковую навигационную панель для быстрого доступа ко всем модулям и центральную рабочую область. Были детально проработаны макеты и логика взаимодействия пользователя для каждого основного функционального экрана: «Главная», «Внедрить», «Извлечь», «Обработка», «Статистика», «Рисование», «Текст в PNG» и «Сравнить», что позволило минимизировать когнитивную нагрузку и сделать интерфейс предсказуемым. Вид одного из диалоговых окон (в режиме внедрения сообщения в текстовый документ-контейнер) и основной функционал приложения показаны на рисунке.



Диалоговое окно приложения в режиме внедрения сообщения на основе метода
Dialog window of the application in message embedding mode based on method

Проектирование модульной структуры приложения было выполнено в соответствии с принципом единой ответственности, что привело к созданию логически изолированных и слабо связанных компонентов. Структура включила описание главного управляющего модуля main.py, который является точкой входа и сервис-провайдером для всего приложения. Выделен специализированный модуль стеганографических алгоритмов stegan.py, полностью отделенный от логики интерфейса,

что упрощает его тестирование и модификацию. Кроме того, для каждого функционального экрана был создан отдельный модуль в директории layouts, инкапсулирующий его представление и логику. Для этих компонентов были четко определены их основные обязанности, ключевые атрибуты, методы и принципы взаимодействия между собой и с внешними библиотеками.

Заключение

Важным аспектом при разработке программного средства являлась не только реализация алгоритмов для внедрения и извлечения информации на основе пользовательских ключей, но и добавление дополнительных модулей, расширяющих его возможности. К таким модулям относятся инструменты для базовой обработки изображений с применением разнообразных фильтров, функции для сбора и визуализации статистических данных об изображениях, возможности простого графического редактирования и генерации изображений из текстовых описаний, а также инструмент для попиксельного сравнения изображений. Эти возможности выгодно отличают разработанное приложение от многих узкоспециализированных стеганографических утилит.

Список использованных источников

1. Савельева, М. Г., Урбанович П. П. (2024) Стеганографическое преобразование на основе модификации полутоновых оттенков растрованных документов. *Информационно-управляющие системы*. 6(133). 2-14.

References

1. Saveleva M. G., Urbanovich P. P. (2024) Steganographic transformation based on the modification of halftone shades of rasterized documents. *Information and Control Systems*. 6(133), 2-14 (in Russian).

Сведения об авторе

Савельева М.Г., ассистент кафедры информационных систем и технологий, учреждение образования «Белорусский государственный технологический университет», saveleva@belstu.by.

Information about the author

Saveleva M. G., Assistant Professor of the Department of Information Systems and Technologies, Educational Institution “Belarusian State Technological University”, saveleva@belstu.by.

УДК 539.216.2:621.317

НЕЛИНЕЙНЫЕ СВОЙСТВА ЧАСТОТНОЙ ЗАВИСИМОСТИ ЕМКОСТИ СТРУКТУР НА ОСНОВЕ ПОЛУПРОВОДНИКОВЫХ ГРАФИТОПОДОБНЫХ ПЛЕНОК УГЛЕРОДА

Д.А. Коваленко, М.С.Х. Аль-Махдави, И.А. Врублевский

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В работе исследованы частотные зависимости емкости структур металл-полупроводник-металл на основе тонких полупроводниковых графитоподобных пленок углерода, осажденных в вакууме. Установлено, что тип частотной кривой емкости не зависит от полярности приложенного напряжения смещения. Обнаружено резкое увеличение емкости на низких частотах и ее уменьшение с последующим насыщением в высокочастотной области. Показано, что наблюдаемые нелинейные особенности могут быть объяснены поляризацией Максвелла-Вагнера, обусловленной наличием проводящих графитоподобных нанокластеров (sp^2 -гибридизация) в диэлектрической матрице (sp^3 -гибридизация). Полученные результаты важны для создания электромагнитных экранов на основе углеродных наноструктурированных материалов.

Ключевые слова: графитоподобные пленки углерода; емкостные свойства; частотная зависимость; поляризация Максвелла-Вагнера; sp^2/sp^3 -гибридизация; нанокластеры; диэлектрическая проницаемость; электрофизические свойства.

NONLINEAR CAPACITANCE-FREQUENCY CHARACTERISTICS OF STRUCTURES WITH SEMICONDUCTING GRAPHITE-LIKE CARBON FILMS

D. A. Kavalenka, M. S. H. Al-Mahdawi, I. A. Vrublevsky

*Educational Institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. The paper investigates the frequency dependences of the capacitance of metal-insulator-metal structures based on thin semiconducting graphite-like carbon films deposited in vacuum. It was found that the type of capacitance frequency curve does not depend on the polarity of the applied bias voltage. A sharp increase in capacitance at low frequencies and its decrease followed by saturation in the high-frequency region were observed. It is shown that the observed nonlinear features can be explained by Maxwell-Wagner polarization due to the presence of conductive graphite-like nanoclusters (sp^2 -hybridization) in a dielectric diamond-like matrix (sp^3 -hybridization). The obtained results are important for understanding the electrophysical properties of carbon nanostructured materials.

Keywords: graphite-like carbon films; capacitive properties; frequency dependence; Maxwell-Wagner polarization; sp^2/sp^3 hybridization; nanoclusters; dielectric constant; thin films; electrophysical properties; carbon nanomaterials.

Введение

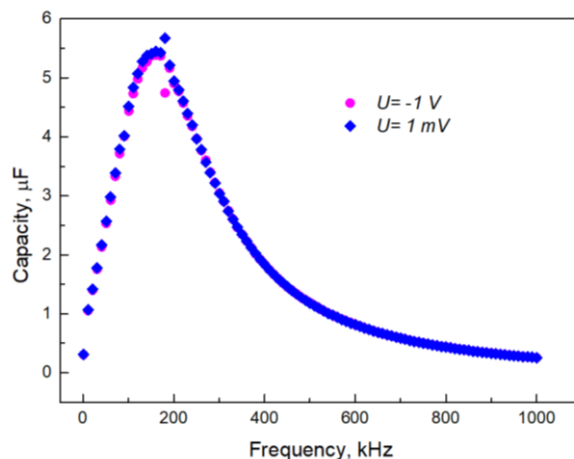
Углерод способен формировать материалы с широким спектром свойств: от диэлектрических (алмаз) до проводящих (графит), что

обусловлено различными типами гибридизации атомов (sp^2 и sp^3). Поэтому тонкие графитоподобные пленки, которые могут сочетать оба типа связей, представляют значительный интерес для электроники и создания электронных фильтров благодаря возможности управления их электрофизическими параметрами. Целью данной работы является исследование частотных зависимостей емкости и анализ механизмов поляризации в структурах на основе таких пленок.

Основная часть

Тонкие графитоподобные углеродные пленки толщиной ~ 50 нм были осаждены в вакууме на стеклянные подложки с нижним слоем никеля. Верхние металлические контакты (Ni) площадью 800×800 мкм формировались методом электронно-лучевого испарения через маску. Измерения емкости проводились с помощью анализатора TH512 и зондовой станции SEMISHARE M6 в широком диапазоне частот при различных полярностях напряжения смещения.

Экспериментально установлено, что частотные зависимости емкости носят нелинейный характер (рисунок). Независимо от полярности приложенного напряжения, на низких частотах наблюдается резкое увеличение емкости, тогда как в высокочастотной области происходит ее спад с последующим насыщением.



Частотная характеристика емкости структур
с полупроводниковой графитоподобной пленкой углерода
Frequency dependence of capacitance of structures
with semiconducting graphite-like carbon film

Подобное поведение характерно для гетерогенных систем и объясняется поляризацией Максвелла-Вагнера. Согласно этому механизму, на границах раздела фаз с различной проводимостью происходит накопление зарядов, что приводит к росту диэлектрической проницаемости на низких частотах. С увеличением частоты вклад данной

поляризации снижается, и диэлектрическая проницаемость стремится к стационарному значению.

В исследуемых графитоподобных пленках роль проводящих включений играют нанокластеры с sp^2 -гибридизацией (графитоподобная фаза), окруженные диэлектрической матрицей с преобладанием sp^3 -связей. Наличие таких наноструктурных неоднородностей подтверждено данными просвечивающей электронной микроскопии.

Заключение

В работе показано, что структуры металл-полупроводник-металл на основе полупроводниковых графитоподобных углеродных пленок обладают ярко выраженной нелинейностью частотной зависимости емкости. Установлено, что доминирующим механизмом, ответственным за высокие значения емкости в низкочастотной области, является поляризация Максвелла-Вагнера. Данный эффект обусловлен наличием проводящих sp^2 -кластеров в диэлектрической sp^3 -матрице. Полученные результаты важны для понимания электрофизических свойств углеродных наноматериалов и их применения для создания электромагнитных экранов.

Список использованных источников

1. Долженко Д. И., Бородзюля В. Ф., Захарова И. Б., Сударь Н. Т. (2021) Влияние тока, ограниченного объемным зарядом, на диэлектрические свойства поликристаллических пленок фуллерита C60. Журнал технической физики. 91 (1), 58–63.
2. Wang Y. J., Li H. X., Ji L., Liu X. H., Wu Y. X., Zhou H. D., et al. (2012) Superior tribological properties of an amorphous carbon film with a graphite-like structure. Chinese Physics B. 21 (1), 016101.

References

1. Dolzhenko D. I., Borodzyulya V. F., Zakharova I. B., Sudar N. T. (2021) [Influence of space-charge-limited current on the dielectric properties of polycrystalline C60 fullerene films]. Zhurnal Tekhnicheskoi Fiziki [Technical Physics Journal]. 91 (1), 58–63. (In Russian).
2. Wang Y. J., Li H. X., Ji L., Liu X. H., Wu Y. X., Zhou H. D., et al. (2012) Superior tribological properties of an amorphous carbon film with a graphite-like structure. Chinese Physics B. 21 (1), 016101.

Сведения об авторах

Коваленко Д.А., инженер-химик НИЛ «Многофункциональные металлооксидные композитные материалы», УО «Белорусский государственный университет информатики и радиоэлектроники», kavalenka.d.a@gmail.com.

Аль-Махдави М.С.Х., аспирант каф. Защиты информации, УО «Белорусский государственный университет информатики и радиоэлектроники».

Врублевский И.А., канд. техн. наук, доц., зав. лаб. НИЛ «Многофункциональные металлооксидные композитные материалы», УО «Белорусский государственный университет информатики и радиоэлектроники», vrublevsky@bsuir.edu.by.

Information about the authors

Kavalenka D. A., Chemical Engineer, Research Laboratory “Multifunctional Metal-Oxide Composite Materials”, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, kavalenka.d.a@gmail.com.

Al-Mahdawi M. S. H., Postgraduate Student, Information Protection Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Vrublezsky I.A., Cand. Sci. (Tech.), Associate Professor, Head of the Research Laboratory “Multifunctional Metal-Oxide Composite Materials”, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, vrublevsky@bsuir.edu.by.

УДК 004.056.5

СОВРЕМЕННАЯ МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

П.Б. Гусаков, К.Е. Макаренко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрены современные методологические подходы к построению систем защиты информации в контексте обеспечения информационной безопасности в Республике Беларусь. Проанализированы основные принципы проектирования интегрированных программ: непрерывность, комплексность, экономическая целесообразность и адаптивность, которые закреплены в национальном законодательстве. Представлена классификация методов защиты. Проанализированы направления развития в области методологии защиты информации в ходе реализации концепции цифрового суверенитета до 2030 г.

Ключевые слова: методы защиты информации; моделирование угроз; криптография; искусственный интеллект в безопасности; инженерно-техническая защита; квантовое шифрование; управление доступом; информационная безопасность.

MODERN METHODOLOGY FOR BUILDING INFORMATION PROTECTION MEANS AND SYSTEMS

P.B. Gusakov, K.E. Makaranka

Educational Institution “Belarusian State University of Informatics and Radio Electronics”, Minsk, Republic of Belarus

Abstract. This article examines modern methodological approaches to building information security systems in the context of information security in the Republic of Belarus. It analyzes the key principles of integrated program design, including continuity, comprehensiveness, economic feasibility, and adaptability, as enshrined in national legislation. A classification of security methods is presented. Development directions in information security methodology are analyzed as part of the implementation of the concept of digital sovereignty by 2030.

Keywords: information protection methods; threat modeling; cryptography; artificial intelligence in security; engineering and technical protection; quantum encryption; access control; information security.

Введение

Актуальность темы данного доклада обусловлена необходимостью совершенствования методологических подходов к построению систем защиты информации в условиях эскалации киберугроз и цифровой трансформации объектов критической инфраструктуры. В Республике Беларусь создана всеобъемлющая правовая база для защиты информации. Ключевыми документами, определяющими государственную политику, выступают Концепция информационной безопасности, утвержденная Постановлением Совета Безопасности № 1 от 18 марта 2019 года, а также Концепция обеспечения суверенитета в сфере цифрового развития до 2030 года, утвержденная Постановлением Совета Министров № 1074 от 31 декабря 2024 года. Данные акты задают вектор развития национальных систем защиты информации в контексте обеспечения информационного суверенитета [1]. В настоящем докладе рассматриваются современные методологические принципы создания СЗИ, классификация методов защиты и перспективные направления развития технологий безопасности с учетом требований национальных регуляторов.

Основная часть

Фундаментальной основой построения системы безопасности является соблюдение принципов, закрепленных в законе Республики Беларусь «Об информации, информатизации и защите информации» № 455-З и подробно изложенных в нормативных документах Оперативно-аналитического центра при Президенте Республики Беларусь.

Принцип непрерывности и надежности защиты подразумевает работу системы безопасности в состоянии постоянной готовности к отражению угроз, временные и пространственные характеристики которых заранее не predetermined. Принцип универсальности обусловлен отсутствием универсальных методов защиты и требует интеграции правовых (регулируемых, в частности, Указом Президента № 422 "О мерах по совершенствованию защиты персональных данных"), организационных, инженерных и программных процедур, обеспечивающих появление системы безопасности. Принцип экономической целесообразности (адекватности) устанавливает взаимосвязь между стоимостью защиты и стоимостью защищаемых информационных активов или возможным ущербом, причиняемым в результате расчетов. Принцип адаптивности (гибкости) особенно важен с методологической точки зрения. Из-за динамичного характера угроз меры безопасности не могут быть статичными. Обнаружение злоумышленником конкретного метода защиты снижает его эффективность, что влечет за собой внедрение механизмов быстрого обновления мер безопасности [2].

Процесс построения системы безопасности регулируется положением о защите технической и криптографической информации (утвержденным Указом Президента Республики Беларусь № 196) и включает в себя следующие этапы:

- детализация предметной области, то есть определение целевых функций системы (контроль доступа, обеспечение конфиденциальности каналов связи, защита от несанкционированного копирования и т.д.);

- построение модели угроз и модели атакующего имеет решающее значение, поскольку позволяет идентифицировать угрозы, связанные с информационной безопасностью. Модель преступника должна учитывать его потенциальные возможности;

- разработка политики безопасности – набора правил и норм, регулирующих обработку информации. Для государственных учреждений, организаций и операторов персональных данных (согласно Закону № 99-3) наличие официальной политики безопасности является обязательным требованием;

- определение структуры и компонентов системы безопасности.

Обобщение и оценка гарантий работоспособности: проверка правильности внедрения механизмов защиты, включая процедуры обязательной сертификации объектов информатики в соответствии с процедурами, установленными ОАЦ.

Современная методология защиты информации предполагает многоуровневый подход, который объединяет различные категории методов.

1. Инженерно-технические методы ЗИ включают в себя создание механических барьеров, организацию зон контролируемого доступа, маскировку каналов утечки информации. Обеспечение физической защиты серверных помещений, аппаратных систем и носителей информации чрезвычайно важно, особенно для критически важных объектов информатизации (КВОИ).

2. Криптографические методы ЗИ. В Республике Беларусь вектор развития смещается в сторону использования национальных стандартов криптографического преобразования и средств, сертифицированных ОАЦ.

3. Программно-аппаратные методы ЗИ. К данной категории методов относятся идентификация, аутентификация и контроль доступа субъектов к информационным ресурсам. Современная методология характеризуется переходом от простых систем паролей к многофакторной аутентификации (MFA), биометрическим технологиям и внедрению концепции нулевого доверия («zero trust»).

Перспективные направления развития методологии обеспечения информационной безопасности:

1. Применение технологий искусственного интеллекта. Искусственный интеллект и системы, основанные на машинном обучении, анализируют закономерности поведения пользователей и сетевой трафик, выявляют аномалии, характерные для атак нулевого дня. Искусственный интеллект был интегрирован в системы SIEM и платформы для автоматизации процессов реагирования на инциденты. Разработка интеллектуальных систем обнаружения вторжений является приоритетным направлением научных исследований [3].

2. Защита облачных сред и распределенных систем

В рамках концепции цифрового суверенитета до 2030 года Беларусь стоит задача по снижению зависимости от зарубежных облачных провайдеров и развитию местной инфраструктуры. Миграция предприятий и организаций в облачную среду создает спрос на методы защиты, которые интегрируются непосредственно в цикл разработки программного обеспечения, что позволяет проверять безопасность кода на этапах его написания и компиляции [3].

Заключение

Таким образом, современная методология построения средств информационной безопасности в Республике Беларусь представляет собой сложную междисциплинарную область, интегрирующую достижения технических наук с императивными требованиями национального законодательства и регулирующих органов. Эффективность средств защиты информации определяется не только использованием передовых технологических решений, но и строгим соблюдением организационных процедур на всех этапах жизненного цикла системы, от моделирования угроз до сертификации ИТ-объекта. Перспективы развития методологии связаны с внедрением адаптивных самообучающихся систем, реализующих концепцию нулевого доверия и обеспечивающих информационный суверенитет государства.

Список использованных источников

1. Голиков В. Ф., Черная И. И., Зельманский О. Б. (2013) Разработка методологии информационной безопасности как основы создания и изучения защищенных информационных систем, 97–98.
2. Конявская С.В. (2013) К вопросу о классификации объектов защиты информации (3), 14–18.
3. Moller P. F. Dietmar, (2025) Cybersecurity for Network and Information Security : Principles, Techniques and Applications.

References

1. Golikov V. F., Chernaya I. I., Zelmansky O. B. (2013) Development of Information Security Methodology as a Basis for Creating and Studying Protected Information Systems, 97–98.
2. Konyavskaya S.V. (2013) Classification of Information Protection Objects (3), 14–18 (in Russian).
3. Moller P. F. Dietmar, (2025) Cybersecurity for Network and Information Security : Principles, Techniques and Applications.

Сведения об авторах

Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Макаренко К.Е., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», makarenkokirilka05@gmail.com.

Information about the authors

Gusakov P.B., Mast., head of the cycle, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Makaranka K.E., student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, makarenkokirilka05@gmail.com.

УДК 004.056

МЕТОДИКА АНАЛИЗА ТРАФИКА И ВЕРИФИКАЦИИ ШИФРОВАНИЯ В СОТОВОЙ СЕТИ 4/5G НА ОСНОВЕ ИМИТАТОРА БАЗОВОЙ СТАНЦИИ ЮНИТЕСС

Д.Н. Одинец

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Статья описывает методику анализа трафика и верификации шифрования, реализованную в имитаторе базовой станции ЮНИТЕСС. Метод базируется на спецификациях 3GPP TS 33.401 и TS 35.201–207. Верификация включает два ключевых этапа: проверку корректности процедур аутентификации и генерации ключей, а также валидацию криптографических алгоритмов. Имитатор принудительно согласовывает алгоритмы защиты, вычисляет эталонные значения и сравнивает их с параметрами, полученными от абонентского устройства, что позволяет выявить ошибки реализации и уязвимости в системе безопасности терминалов 4/5G.

Ключевые слова: имитатор базовой станции ЮНИТЕСС; безопасность данных; шифрование; перехват сигнала; аутентификация.

METHOD OF TRAFFIC ANALYSIS AND ENCRYPTION VERIFICATION IN A 4/5G CELLULAR NETWORK BASED ON THE UNITESS SIMULATOR OF BASE STATION

D.N. Adzinets

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The article describes the method of traffic analysis and encryption verification implemented in the UNITESS base station simulator. The method is based on the 3GPP TS 33.401 and TS 35.201-207 specifications. Verification includes two key stages: verification of the correctness of authentication and key generation procedures, as well as validation of cryptographic algorithms. The simulator forcibly coordinates protection algorithms, calculates reference values and compares them with the parameters received from the subscriber device, which allows you to identify implementation errors and vulnerabilities in the security system of 4/5G terminals.

Keywords: UNITESS base station simulator; data security; encryption; signal interception; authentication.

Введение

Современные устройства с поддержкой GSM, LTE и 5G передают конфиденциальную информацию: телеметрию промышленных объектов, персональные данные, финансовые транзакции, команды управления критической инфраструктурой. В условиях роста киберугроз недостаточно проверить, работает ли модуль связи, необходимо убедиться, что он защищает данные – даже при целенаправленной атаке. Даже если модуль успешно проходит функциональное тестирование, скрытая уязвимость в реализации протоколов безопасности может сделать устройство мишенью для злоумышленников. Выявление таких дефектов на этапе производства – единственный способ избежать репутационных и финансовых потерь после отгрузки.

Методика анализа трафика и верификации шифрования

Для проверки реализации механизмов защиты необходим полный контроль над параметрами сети. Реальные операторские сети не позволяют реализовать требования предложенной методики тестирования.

1. Принудительно включать / выключать конкретные алгоритмы шифрования.

2. Модифицировать сигнальные сообщения «на лету».

3. Эмулировать атаки в изолированной среде.

Имитатор базовой станции ЮНИТЕСС решает эту задачу, предоставляя лабораторную среду с поддержкой полного стека протоколов 3GPP и алгоритмов безопасности: AES, Snow3G и ZUC для шифрования

и проверки целостности. Методика предполагает создание изолированной лабораторной 4/5G сети (без выхода в публичный интернет) и применение ЮНИТЕСС АРМ для автоматизации сценариев и сбора логов.

В процессе тестов имитируются представленные в таблице атаки.

Виды имитируемых атак
Types of simulated attacks

Тип атаки	Метод эмуляции	Критерий прохождения
Downgrade-атака	Имитатор предлагает только устаревшие или незащищенные алгоритмы (например, нулевое шифрование)	Модуль отвергает конфигурацию, если она ниже минимального порога безопасности, заданного в политике устройства
Replay-атака	Повторная отправка ранее записанных зашифрованных пакетов данных	Модуль игнорирует дубликаты благодаря механизмам счетчиков последовательностей (HFN/SQN)
Перехват идентификаторов	Анализ процедуры первичного подключения: передается ли постоянный идентификатор в открытом виде	Модуль использует временные идентификаторы (TMSI/GUTI) или зашифрованный SUCI; IMSI/SUPI не передается в открытом эфире
Атака на хэндовер	Эмуляция передачи контекста безопасности между «сота́ми» с подменой ключей	Ключи корректно обновляются (Key Derivation), сессия не прерывается, данные не передаются в открытом виде

Для различных классов устройств существуют свои особенности тестирования. Например, для IoT-датчики (умный город, ЖКХ) тестируется защита телеметрии, устойчивость к подмене команд, для промышленных контроллеров: гарантия подлинности команд управления, защита от несанкционированного доступа. Для транспортных терминалов тестируются конфиденциальность геоданных, защита от отслеживания. Для медицинских устройств важно протестировать соответствие требованиям защита персональных данных.

Ключевым преимуществом методики является возможность принудительного выбора алгоритмов шифрования (AES, Snow3G, ZUC), модификации сигнальных сообщений и эмуляции широкого спектра атак, включая downgrade-атаки, повторную передачу пакетов (replay), перехват идентификаторов и подмену ключей при хэндовере. Такой подход позволяет выявить скрытые дефекты реализации протоколов безопасности 3GPP (TS 33.401, TS 35.201–207) на этапе производства или лабораторных испытаний, тем самым предотвращая потенциальные репутационные и финансовые потери, связанные с эксплуатацией уязвимых устройств.

Особую ценность представляет адаптивность методики под различные классы оборудования – от IoT-датчиков до промышленных

контроллеров и медицинской техники, – что подтверждает ее универсальность. Внедрение данной методики в процессы контроля качества позволяет гарантировать не только работоспособность устройств, но и их способность противостоять целенаправленным атакам, обеспечивая конфиденциальность, целостность и подлинность передаваемых данных [1].

Заключение

Предложенная методика анализа трафика и верификации шифрования на базе имитатора базовой станции ЮНИТЕСС представляет собой комплексное решение для оценки защищенности устройств связи стандартов GSM, LTE и 5G. В условиях растущих киберугроз, нацеленных на перехват конфиденциальной информации и нарушение целостности управления критическими объектами, традиционное функциональное тестирование становится недостаточным. Использование имитатора позволяет воссоздать изолированную тестовую среду с полным контролем параметров сети, что недостижимо в условиях реальной операторской инфраструктуры.

Список использованных источников / References

1. Adzinets Dzmitry. Testing GSM/LTE/5G modules in conditions of no or unstable cellular communication. LXXIV International Multidisciplinary Conference “Recent Scientific Investigation”. Proceedings of the Conference (12-13 November, 2025). Primedia E-launch LLC, Shawnee, USA. 2025. 122 p., p.47-50.

Сведения об авторе

Одинец Д.Н., канд. техн. наук, доцент, доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», adzinets@bsuir.by.

Information about the author

Adzinets D., Dr. Sci. (Tech.), Associate Professor, Associate Professor, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, adzinets@bsuir.by.

УДК 004.72:004.56

МЕТОД ПРЕДОТВРАЩЕНИЯ УГРОЗ В ЗАКРЫТОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЕ НА ОСНОВЕ ВНУТРЕННЕЙ СЕГМЕНТАЦИИ

В.В. Чиж

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Предложен метод предотвращения распространения вредоносного кода в закрытой сетевой инфраструктуре на основе внутренней сегментации и внутренних сегментирующих межсетевых экранов (*Internal Segmentation Firewall, ISFW*). Сеть делится на изолированные сегменты безопасности с централизованным управлением доступов. Контроль трафика позволяет ограничить латеральное перемещение атакующего при компрометации одного узла. Приводится упрощенная модель оценки вероятности успешного распространения атаки и текстовое описание блок-схемы закрытой сетевой инфраструктуры.

Ключевые слова: закрытая сеть; межсетевой экран; латеральное перемещение; модель угроз.

METHOD FOR PREVENTING THREATS IN A CLOSED NETWORK INFRASTRUCTURE BASED ON INTERNAL SEGMENTATION

V.V. Chizh

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. A method for preventing the spread of malicious code in a closed network infrastructure based on internal segmentation and Internal segmentation firewalls (ISFW) is being considered. The network is divided into isolated security segments with centralized access control. Traffic control allows you to limit the lateral movement of an attacker when one node is compromised. A simplified model for estimating the probability of successful spread of an attack and a text description of a block diagram of a closed network infrastructure are provided.

Keywords: closed network; firewall; lateral movement; threat model.

Введение

Закрытые сетевые инфраструктуры считаются более защищенными из-за отсутствия прямого подключения к интернету, однако многие атаки реализуются через внутренние узлы: ошибки администрирования, уязвимости приложений и компрометацию учетных записей. Для критических систем это создает риск быстрого выхода злоумышленника на серверы управления технологическими процессами и базы данных.

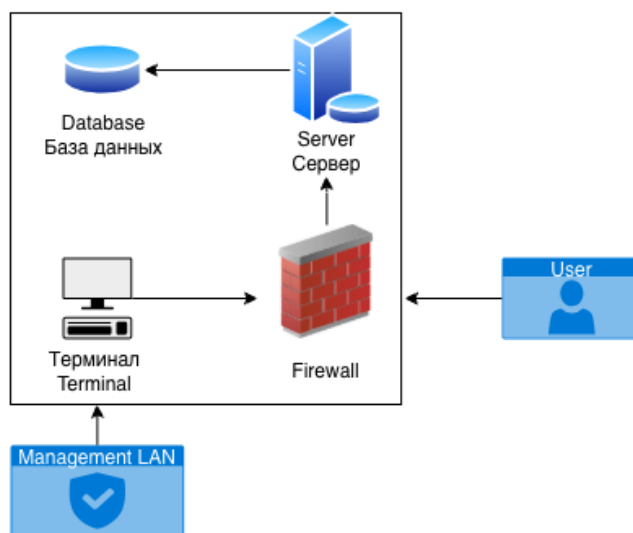
Цель – описать метод предотвращения распространения вредоносного кода в закрытой сети на основе такой сегментации.

Основная часть

Рассматривается латеральное распространение вредоносного ПО после компрометации одной рабочей станции в офисном сегменте. Цель несанкционированного доступа: получить управление к сегментам, где размещены сервера приложений, базы данных и системы управления. Предполагается логическое разделение сети на несколько подсетей, наличие критических и некритических сегментов, а также отсутствие прямого доступа в интернет при наличии контролируемых шлюзов. Задача защиты – уменьшить вероятность перехода из некритического в критический сегмент без потери необходимой функциональности.

Внутренняя сегментация – это разбиение сети на сегменты безопасности, взаимодействие между которыми разрешено только по заранее определенным правилам. Для реализации используются внутренний сегментирующий межсетевой экран, установленный на стыке виртуальной сети. Он фильтрует межсегментный трафик, применяют анализ пакетов и поведенческое обнаружение вредоносной активности, контролируя трафик не только на периметре, но и между внутренними сегментами.

Упрощенная структура закрытой сети с внутренней сегментацией приведена на рисунке.



Структурная схема закрытой сетевой инфраструктуры с внутренней сегментацией
Block diagram of a closed network infrastructure with internal segmentation

Метод включает: аналитическое выделение сегментов и критических ресурсов; проектирование модели сегментации и точек установки внутренних экранов; организацию централизованного мониторинга и оперативной изоляции подозрительных сегментов [1, 2].

Заключение

Предложенный метод внутренней сегментации и применения внутренних сегментирующих межсетевых экранов позволяет ограничить распространение вредоносного кода в закрытой сети и снизить вероятность достижения критических сегментов при успешной компрометации одного узла. Упрощенная модель показывает, что увеличение количества контролируемых межсегментных переходов и улучшение качества настроек политик приводит к уменьшению вероятности успешной атаки. Данный подход особенно полезен для сетей критической инфраструктуры и может быть адаптирован под конкретные архитектуры и регуляторные требования.

Список использованных источников

1. Альравашде К., Перди С. Формальный подход к сегментации сети. Компьютеры и безопасность (2021), 99–102.
2. Ранжирование объектов критической информационной инфраструктуры сотовых сетей. Вестник Алтайской академии экономики и права (2023), 324–334.

References

1. Alrawashdeh K., Purdy C. A Formal Approach to Network Segmentation. Computers & Security (2021), 99–102.
2. Ranking of objects of critical information infrastructure of cellular networks. Bulletin of the Altai Academy of Economics and Law (2023), 324–334.

Сведения об авторе

Чиж В.В., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vik220011@gmail.com.

Information about the author

Chizh V., master's student at the Information Protection Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, vik220011@gmail.com.

УДК 004.056.5

ПОСТРОЕНИЕ ДОВЕРЕННОЙ СРЕДЫ ИСПОЛНЕНИЯ НА БЕЛОРУССКИХ ПРЕДПРИЯТИЯХ

А.А. Ярмольчик, П.Б. Гусаков

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается концепция построения доверенной среды исполнения (Trusted Execution Environment) как современного подхода к обеспечению технической защиты информации на белорусских предприятиях. Проведен анализ международных практик организации безопасных сред, включая Trusted Research Environments и концепцию «Пяти гарантий безопасности». Обоснована необходимость перехода от традиционной модели защиты периметра к созданию контролируемых доверенных сред для обеспечения устойчивости организаций, работающих с конфиденциальной информацией.

Ключевые слова: Доверенная среда исполнения, Trusted Execution Environment, техническая защита информации, изоляция, проектирование, аудит, безопасность, белорусские предприятия, конфиденциальность, интеграция.

BUILDING A TRUSTED EXECUTION ENVIRONMENT AT BELARUSIAN ENTERPRISES

A.A. Yarmolchik, P.B. Gusakov

*Educational institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. This article examines the concept of building a Trusted Execution Environment as a modern approach to ensuring technical information security at Belarusian enterprises. It analyzes international practices for creating secure environments, including Trusted Research Environments and the "Five Security Guarantees" concept. The need to transition from the traditional perimeter security model to the creation of controlled trusted environments to ensure the resilience of organizations handling confidential information is substantiated.

Keywords. Trusted Execution Environment, technical information security, isolation, design, audit, security, Belarusian enterprises, confidentiality, integration.

Введение

В современном мире, характеризующемся стремительной цифровой трансформацией всех сфер деятельности, вопросы обеспечения технической защиты информации выходят на передний план для организаций любого масштаба. Белорусские предприятия, функционирующие в условиях необходимости адаптации к новым геополитическим и технологическим вызовам, сталкиваются с потребностью пересмотра подходов к построению своих информационных систем. Традиционная модель защиты, основанная на создании жесткого периметра вокруг корпоративной сети, постепенно уступает место более гибким и надежным

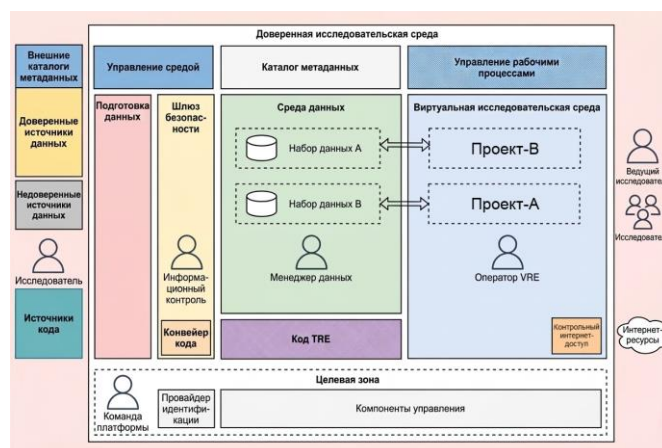
архитектурам. Одной из таких перспективных концепций является построение Trusted Execution Environment (доверенной среды исполнения) – контролируемого пространства, предназначенного для безопасной обработки, хранения и анализа конфиденциальных данных и работы критически важных приложений. В условиях роста числа киберугроз, внедрение принципов доверенных сред становится необходимостью для обеспечения устойчивости и информационной безопасности белорусского бизнеса и государственных учреждений.

Основная часть

Само понятие Trusted Execution Environment (TEE) не является абсолютно новым и имеет различные интерпретации в мировой практике. В международном контексте широкое распространение получили Trusted Research Environments (TRE) или безопасные среды для работы с данными, которые активно применяются в Великобритании и других странах для организации доступа исследователей к чувствительным медицинским и статистическим данным без риска их утечки. Ключевым принципом организации таких сред является концепция «Пяти гарантий безопасности» (Five Safes), разработанная Службой национальной статистики Великобритании. Эта концепция подразумевает обеспечение безопасности на пяти уровнях: безопасные люди (Safe people), безопасные проекты (Safe projects), безопасные данные (Safe data), безопасные настройки среды (Safe settings) и безопасные выходные результаты (Safe outputs) [1]. Данный подход позволяет реализовать среду, в которой исследователь получает доступ к вычислительным мощностям и данным в защищенном периметре, но не может несанкционированно скопировать информацию вовне. Применение подобных архитектурных решений, например, на базе облачных платформ, позволяет использовать передовые сервисы безопасности для соответствия строгим требованиям управления данными.

На рисунке показаны типичные элементы, обычно встречающиеся в TRE. Однако для белорусских предприятий особый интерес представляет иная грань понятия доверенной среды, а именно техническая реализация Trusted Execution Environments – доверенных сред исполнения на аппаратном и системном уровне. TEE представляют собой изолированные области на процессоре или в системе, гарантирующие защиту кода и данных даже в случае компрометации основной операционной системы [2]. Эти технологии, включающие аппаратные решения от различных производителей, направлены на обеспечение доверенной загрузки, изоляцию критически важных вычислений и защиту памяти от несанкционированного доступа. Методы построения таких сред основываются на расширении классической цепочки доверия от аппаратного обеспечения до прикладного программного обеспечения,

что позволяет гарантировать целостность исполняемого кода и конфиденциальность обрабатываемых данных даже на потенциально скомпрометированной платформе. Применение таких технологий критически важно для защиты ключевых систем белорусских предприятий, обрабатывающих персональные данные, коммерческую тайну или иную чувствительную информацию.



Функциональная архитектура TRE
Functional architecture of TRE

Процесс проектирования и аудита ТРЕ для предприятия должен учитывать всю совокупность этих факторов – от глобальных концепций безопасности до локальных нормативных требований и интеграционных задач. Доверенная среда – это не единичное устройство или программа, а комплексное организационно-техническое решение. Как следует из спецификации SATRE (Standardised Architectures for Trusted Research Environments), разработанной при участии многих организаций, успешная реализация TRE требует рассмотрения не только технологических компонентов, но и управленческих процессов, ролей пользователей, процедур контроля доступа и управления. Применительно к белорусским реалиям, построение такой среды должно начинаться с детального аудита существующих информационных активов и бизнес-процессов, определения категорий данных, требующих максимальной защиты, и моделирования угроз. На этапе проектирования необходимо выбрать архитектурный шаблон – будет ли это изолированная среда исполнения для конкретного критического приложения, виртуальная исследовательская среда для работы с базами данных, либо же комплексная система защиты всего предприятия, основанная на принципах нулевого доверия. Ключевым элементом здесь является интеграция с существующей инфраструктурой и используемыми средствами защиты информации, включая сертифицированные в Беларуси средства криптографической защиты и межсетевые экраны.

Заключение

Построение ТЕЕ на белорусских предприятиях представляет собой многогранную задачу, лежащую на стыке передовых мировых практик организации безопасных сред, региональных интеграционных инициатив в рамках ЕАЭС и жестких требований национального законодательства в области технической защиты информации. Переход от концепции защиты периметра к созданию контролируемых, изолированных и верифицируемых сред исполнения является закономерным ответом на усложнение ландшафта угроз и повышение требований к сохранности конфиденциальных данных. Дальнейшее развитие данного направления будет неразрывно связано как с совершенствованием аппаратных платформ и методов изоляции, так и с гармонизацией нормативной базы на национальном и наднациональном уровне, что позволит создавать по-настоящему надежные и функциональные доверенные цифровые пространства.

Список использованных источников / References

1. Amazon Web Services [Electronic resource]. URL: <https://aws.amazon.com>.
2. Shepherd C., Markantonakis K. (2024) *Trusted Execution Environment*.

Сведения об авторах

Ярмольчик А.А., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexey24yarmolchik02@gmail.com.

Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Yarmolchik A.A., Cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, alexey24yarmolchik02@gmail.com.

Gusakov P.B., Master's Degree, Head of Cycle, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

УДК 004.312

МЕТОД ПОВЫШЕНИЯ УНИКАЛЬНОСТИ АППАРТНЫХ ИДЕНТИФИКАТОРОВ ПЛИС НА ОСНОВЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ТИПА КОНФИГУРИРУЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

Л.А. Бурко, А.А. Иванюк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь

Аннотация. В работе рассматривается задача повышения уникальности аппаратных идентификаторов ПЛИС, которые формируются на основе физически неклонировуемых функций типа конфигурируемого кольцевого осциллятора. Показано, что использование аддитивного скремблера для постобработки идентификаторов может приводить к возникновению совпадающих значений вследствие особенностей исходных идентификаторов и начального состояния генератора. Для устранения данной проблемы предложен метод предварительного преобразования исходных идентификаторов. Проведенные экспериментальные исследования показали повышение статистического разнообразия идентификаторов и снижение вероятности коллизий.

Ключевые слова: ПЛИС; ФНФ; ККО; аддитивный скремблер; идентификация; LFSR; переключаемость; защита аппаратуры; расстояние Хэмминга.

METHOD FOR INCREASING THE UNIQUENESS OF FPGA HARDWARE IDENTIFIERS BASED ON PHYSICALLY UNCLONABLE FUNCTIONS OF CONFIGURABLE RING OSCILLATORS

L.A. Burko, A.A. Ivaniuk

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. This article examines the problem of increasing the uniqueness of hardware identifiers for FPGA devices generated using physically unclonable functions based on configurable ring oscillators. Using an additive scrambler for identifier postprocessing can lead to collisions due to the characteristics of the original identifiers and the initial state of the generator. To overcome this issue, a method for pre-transforming the original identifiers is proposed. Experimental studies have demonstrated an increase in the statistical diversity of identifiers and a reduction of collisions.

Keywords: FPGA; PUF; CRO; additive scrambler; identification; LFSR; switching activity; hardware protection; Hamming distance.

Введение

Аппаратные методы обеспечения безопасности играют важную роль в современных информационно-телекоммуникационных системах. Их используют при реализации вычислительных и криптографических функций наряду с программными механизмами защиты информации, что позволяет повысить уровень доверия к устройствам и предотвратить несанкционированное вмешательство. Одной из ключевых задач в области защиты информации является идентификация и аутентификация аппаратных компонентов. Особую актуальность эта задача приобретает для устройств, реализованных на базе ПЛИС, широко применяемых в системах обработки сигналов, телекоммуникационном оборудовании, встроенных вычислительных системах и средствах криптографической защиты информации благодаря высокой гибкости архитектуры и возможности динамической реконфигурации. Программируемая природа таких устройств создает риски подмены аппаратных модулей,

клонирования устройств или внедрения несанкционированных модификаций в конфигурацию системы.

Эффективным способом повышения уровня защищенности аппаратных платформ является использование уникальных аппаратных идентификаторов [1, 2]. В отличие от идентификаторов, хранящихся в энергонезависимой памяти, они могут формироваться на основе внутренних характеристик микросхемы, что существенно усложняет копирование или подмену устройств.

Основная часть

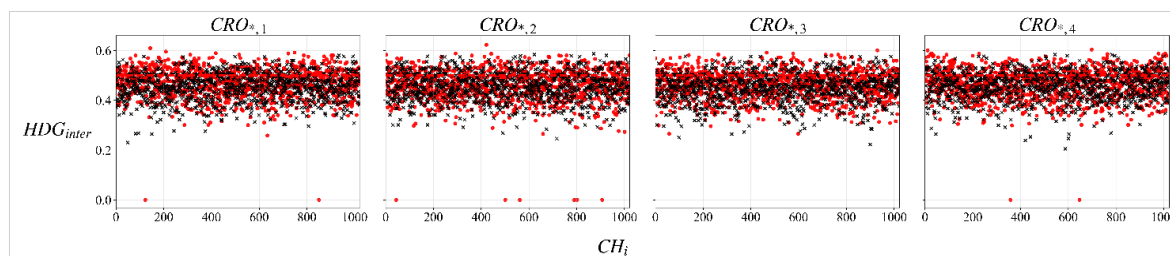
Процесс формирования идентификаторов на базе физически неклонлируемых функций (ФНФ) для ПЛИС был подробно описан в [2]. Степень различия идентификаторов оценивается на основе метрики геометрического среднего расстояний Хэмминга. Эксперимент был проведен на четырех различных ПЛИС, на каждой из которых было реализовано по четыре экземпляра ФНФ ККО с фиксированными параметрами, которые влияют на длину идентификатора. Полученные идентификаторы различны, но их статистические характеристики остаются недостаточными для обеспечения требуемого уровня метрики уникальности. Была предложена схема улучшения идентификаторов на основе аддитивного скремблера. При оценке уникальности идентификаторов после постобработки возникла проблема появления повторяющихся идентификаторов.

Новое значение идентификатора ID_i^* генерируется при помощи аддитивной схемы путем применения операции хог между первоначальным значением идентификатора ID_i и начальным значением LFSR, входящего в состав скремблера. Разрядность LFSR n совпадает с длиной идентификатора. Важно, чтобы инициализирующее значение генератора было уникальным для каждой пары ПЛИС – ФНФ ККО, поэтому оно формируется путем конкатенации бинарных представлений индексов компонентов (ПЛИС и ФНФ ККО) расширенное нулями до размера n . Например, для ПЛИС с индексом 2 и ФНФ ККО с индексом 3 начальное значение – 000010|0000011. Так как начальные значения содержат большую часть нулей, необходимо осуществить дополнительных K сдвигов LFSR в режиме генератора ($K > n$), таким образом получится новое значение $LFSR_i$.

Пусть даны ID_1 и ID_2 , $LFSR_1$ и $LFSR_2$. Если $ID_1 \oplus LFSR_1 = ID_2 \oplus LFSR_2$, то значение метрики уникальности будет равняться 0. Например, $ID_1 = 110\underline{1}00\underline{0}01\underline{1}000$ и $ID_2 = 110\underline{0}00\underline{1}01\underline{0}000$, $LFSR_1 = 110\underline{1}01\underline{0}00\underline{0}001$ и $LFSR_2 = 110\underline{0}01\underline{1}00\underline{1}001$, отличительные позиции одинаковые. Из-за наблюдаемой коллизии между значениями идентификаторов и значениями LFSR получится нулевое значение метрики уникальности. Способом увеличения расстояния между идентификаторами является их

преобразование в последовательности переходов между соседними битами. Каждая пара заменяется по правилу: $00 \rightarrow 0$, $01 \rightarrow 1$, $10 \rightarrow 1$, $11 \rightarrow 0$. Применяв это, получаются новые начальные идентификаторы 0111000101001 и 0100011110001, отличные на 6 разрядов. После применения аддитивного скремблера получатся значения идентификаторов 1010010101000 и 1000000111000.

В эксперименте было использовано $K = 50$ и измерялась межкристальная уникальность. Красные точки – значения уникальности для идентификаторов после аддитивной схемы без стартовых модификаций, черные крестики – с стартовой модификацией. Общее количество нулевых значений снизилось с 10 до 0. Среднее значение метрики уникальности новых идентификаторов по сравнению с начальными выросло с 0,4023 до 0,4530 (максимальное значение 0,5).



Значения метрик уникальности для идентификаторов
Uniqueness metric values for identifiers

Заключение

Формирование уникальных идентификаторов на аппаратном уровне позволяет повысить устойчивость ПЛИС к атакам, связанным с копированием или подменой устройств. В работе предложен улучшенный подход к генерации уникальных идентификаторов, основанный на предварительном преобразовании исходных идентификаторов на основе переходов между соседними битами перед их использованием в аддитивном скремблере. Это позволяет увеличить различие между начальными последовательностями, что приводит к повышению статистического разнообразия генерируемых идентификаторов и снижению вероятности возникновения совпадающих значений.

Список использованных источников

1. Иванюк, А. А., Бурко Л.А. (2025) Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого. *Информатика*. 22(4) 65–81.
2. Ivaniuk, A., Burko L. (2025) Unclonable Identification and True Random Number Generation Based on CRO PUF. *Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference*, 103-107.

References

1. Ivaniuk, A. A., Burko L.A. (2025) Generation of deterministic identifiers and random numbers using a configurable ring oscillator circuit. *Informatics*. 22(4), 65–81 (in Russian).
2. Ivaniuk, A., Burko L. (2025) Unclonable Identification and True Random Number Generation Based on CRO PUF. *Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference*, 103-107.

Сведения об авторах

Бурко Л.А., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», burkoliana@gmail.com.

Иваниук А.А., д.т.н., профессор кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ivaniuk@bsuir.by.

Information about the authors

Burko L.A., Master Student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", burkoliana@gmail.com.

Ivaniuk A.A., D.Sci, Professor of Informatics Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ivaniuk@bsuir.by.

УДК 004.056.55

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Д.С. Серкевич, Ю.О. Герман

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной статье рассмотрены методы защиты информации с использованием стеганографии, а также предложен вариант для стеганографического скрывания текстовой информации, реализующий метод обратимого сокрытия текстовой информации в изображениях формата JPEG с использованием техники замены наименьшего значащего бита. Представлена актуальность развития методов стеганографии в сфере кибербезопасности.

Ключевые слова: стеганография; LSB; JPEG; цифровые изображения; DCT; RGB; энтропийное кодирование.

STEGANOGRAPHIC METHOD OF INFORMATION PROTECTION

D.S. Serkevich, Yu.O. German

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Abstract. This article examines methods of protecting information using steganography and proposes a method for steganographic concealment of text information, implementing a method for reversibly concealing text information in JPEG images using the least significant bit substitution technique. The relevance of developing steganographic methods in the field of cybersecurity is presented.

Keywords: steganography; LSB; JPEG; digital images; DCT; RGB; entropy coding.

Введение

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. Основная цель стеганографии – скрыть сам факт передачи сообщения, в отличие от криптографии, которая шифрует содержание, но не скрывает саму передачу. Цифровые изображения являются одними из наиболее распространенных контейнеров для стеганографического встраивания информации благодаря их широкому распространению и избыточности данных. Формат JPEG, будучи наиболее популярным форматом для хранения и передачи фотографических изображений, представляет особый интерес для исследователей и разработчиков стеганографических систем.

Основная часть

Метод LSB является одним из наиболее простых и распространенных алгоритмов стеганографии. Он основан на замене младших битов в битовом представлении значений цветовых компонент пикселей изображения битами скрываемого сообщения.

Каждый пиксель цифрового изображения в цветовой модели RGB представлен тремя байтами, соответствующими интенсивности красного, зеленого и синего каналов. Изменение наименьшего значащего бита каждого канала приводит к изменению яркости цвета, что для человеческого глаза остается практически незаметным. Вклад наименее значимого бита в цвет пикселя незначителен, однако при реверсировании порядка битов в байте его роль становится важной.

Формат JPEG использует сжатие с потерями, основанное на дискретном косинусном преобразовании (DCT).

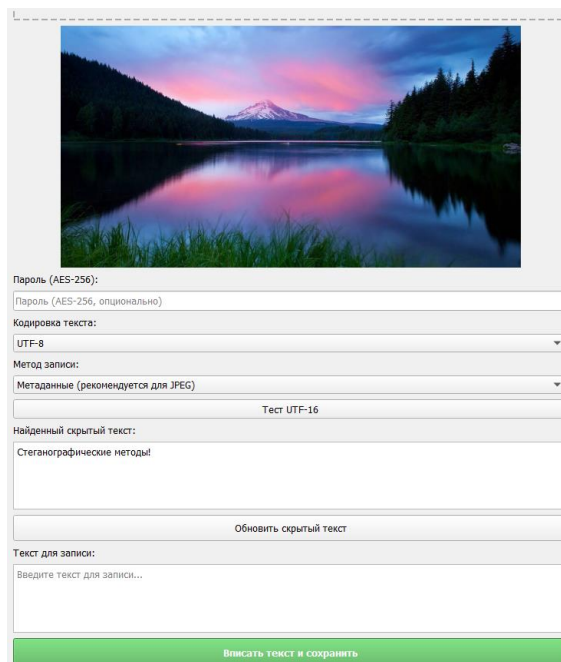
Процесс сжатия включает следующие этапы: преобразование цветового пространства RGB в YCbCr; разбиение изображения на блоки 8×8 пикселей; применение дискретного косинусного преобразования к каждому блоку; квантование DCT-коэффициентов; энтропийное кодирование.

Важной особенностью *JPEG* является то, что при повторном сохранении изображения происходит повторное квантование DCT-коэффициентов, что может разрушить встроенную информацию. Поэтому стеганографические системы для *JPEG* должны либо работать с DCT-коэффициентами до этапа квантования, либо учитывать особенности повторного сжатия.

Разработанное программное обеспечение имеет модульную архитектуру, включающую следующие компоненты:

- 1) модуль работы с изображениями – отвечает за загрузку, обработку и сохранение изображений с сохранением метаданных;
- 2) модуль кодирования – реализует алгоритмы встраивания текста в *LSB* пикселей;
- 3) модуль декодирования – извлекает скрытую информацию из изображения;
- 4) модуль шифрования – обеспечивает дополнительную защиту сообщения с использованием симметричного шифрования;
- 5) графический интерфейс – предоставляет удобные средства взаимодействия с пользователем (рисунок).

Такая архитектура обеспечивает гибкость, возможность независимого тестирования компонентов и легкость.



Графический интерфейс, разработанного программного обеспечения
Graphical interface of the developed software

Заключение

В данной статье были рассмотрены некоторые из основных методов стеганографии изображений для временной области и преобразования области определения. В процессе создания приложения были изучены теоретические основы стеганографии, проведен сравнительный анализ с криптографией, а также детально рассмотрены особенности представления графических данных в формате JPEG и влияние процесса сжатия с потерями на возможность встраивания конфиденциальных данных.

Реализованная модульная архитектура позволила эффективно разделить функционал по работе с изображениями, кодированию и декодированию сообщений, а также обеспечить дополнительную защиту информации путем ее предварительного шифрования. Разработанный графический интерфейс делает инструмент доступным для пользователя.

Список использованных источников

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. (2009) *Цифровая стеганография. Аспекты защиты*. Москва, Издательство «Солон-Пресс».
2. Окатов А.В. (2016) *Методы цифровой стеганографии*. Санкт-Петербург, Издательство «ГУАП».

References

1. Gribunin V.G., Okov I.N., Turintsev I.V. (2009) *Digital Steganography: Security Aspects*. Moscow, Solon-Press Publishing House (in Russian).
2. Okatov A.V. (2016) *Methods of digital steganography*. St. Petersburg, GUAP Publishing House (in Russian).

Сведения об авторах

Серкевич Д.С., магистрант, кафедра защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», sdasha695@gmail.com.

Герман Ю.О., кандидат технических наук, доцент, доцент кафедры информационных технологий автоматизированных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», jgerman@bsuir.by.

Information about the authors

Serkevich D.S., student, Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sdasha695@gmail.com.

German Yu.O., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", jgerman@bsuir.by.

УДК 004.056.53

АЛГОРИТМ ВСТРАИВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА, УСТОЙЧИВЫЙ К ГЕОМЕТРИЧЕСКИМ АТАКАМ И ЗАШУМЛЕНИЮ

И.В. Маутин

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье предложен неслепой алгоритм встраивания цифровых водяных знаков для защиты авторских прав на изображения. Метод базируется на дискретном вейвлет-преобразовании и алгоритме расширения спектра. Криптографическая стойкость обеспечивается использованием хаотических отображений для генерации координат, а устойчивость к геометрическим и шумовым атакам – преобразованием Арнольда и избыточным кодированием с мягким мажоритарным декодированием. Экспериментальные результаты подтверждают высокую эффективность метода.

Ключевые слова: цифровой водяной знак; стеганография; дискретное вейвлет-преобразование; метод расширения спектра; хаотические отображения; преобразование Арнольда; избыточное кодирование; мажоритарное декодирование; защита авторских прав; устойчивость к атакам.

DIGITAL WATERMARKING ALGORITHM ROBUST TO GEOMETRIC AND NOISE ATTACKS

I.V. Mautsin

*Educational Institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. This paper proposes a non-blind digital watermarking algorithm for image copyright protection. The method is based on the discrete wavelet transform and the spread spectrum approach. Cryptographic security is provided by utilizing chaotic maps for coordinate generation, whereas robustness against geometric and noise attacks is achieved through the Arnold transform and repetition coding combined with soft majority decoding. Experimental results confirm the high effectiveness of the proposed method.

Keywords: digital watermark; steganography; discrete wavelet transform; spread spectrum; chaotic maps; Arnold transform; repetition coding; majority decoding; copyright protection; robustness.

Введение

Разработка алгоритмов скрытого внедрения цифровых водяных знаков (ЦВЗ) требует соблюдения баланса между незаметностью, устойчивостью к искажениям и криптографической стойкостью. Частотные методы на базе дискретного вейвлет-преобразования (DWT) демонстрируют высокую устойчивость к компрессии, однако часто остаются уязвимыми к геометрическим атакам и тривиальны для взлома при использовании стандартных генераторов последовательностей. Целью

данной работы является решение проблемы уязвимости частотных ЦВЗ к локальным разрушениям сигнала и импульсному шуму.

Основная часть

Для устранения пространственной корреляции пикселей и защиты от локальных выбросов к матрице ЦВЗ применяется дискретное двумерное преобразование Арнольда [1]. Полученная двумерная матрица линейаризуется в одномерный битовый вектор W длиной L . На втором этапе к вектору W применяется помехоустойчивое кодирование с повторением. Каждый бит w_i дублируется R раз, где R – нечетный коэффициент избыточности, например, $R = 5$ или $R = 7$). Формируется расширенная последовательность W' длиной $L \times R$.

Для обеспечения криптографической стойкости алгоритма координаты встраивания формируются псевдослучайным образом с использованием хаотических отображений [2]. Процесс инициализируется секретным ключом пользователя, который подвергается криптографическому хешированию. Полученный хеш разбивается на блоки, значения которых выступают в качестве начальных условий (x_0, y_0) и управляющих параметров для многомерной хаотической системы. Результатом работы генератора является массив уникальных пар индексов блоков (r, c) . Строгая чувствительность хаотических систем к начальным условиям гарантирует, что изменение ключа даже на один бит приводит к генерации стохастически независимой карты координат, что делает несанкционированное извлечение ЦВЗ вычислительно невыполнимым.

Канал яркости исходного изображения подвергается DWT заданного уровня. Для модификации выбираются коэффициенты среднечастотных поддиапазонов, так как изменения в низких частотах приводят к видимым визуальным артефактам, а высокочастотные детали уничтожаются при компрессии.

Внедрение битов расширенной последовательности W' в выбранные хаотическим генератором координаты (r, c) выполняется по аддитивной схеме метода расширения спектра. Правило модификации вейвлет-коэффициента C математически описывается следующим образом:

$$C'_{r,c} = \begin{cases} C_{r,c} + \alpha, & \text{если } w_i = 1 \\ C_{r,c} - \alpha, & \text{если } w_i = 0 \end{cases}, \quad (1)$$

где $C_{r,c}$ – исходный вейвлет-коэффициент, α – коэффициент силы встраивания, w_i – бит последовательности W' .

Для извлечения ЦВЗ оригинальное и анализируемое изображения подвергаются DWT. С использованием ключа пользователя заново генерируется идентичная хаотическая карта координат. По заданным позициям вычисляется $\Delta C_{r,c} = C^*_{r,c} - C_{r,c}$. Массив значений ΔC разбивается

на блоки длиной R , внутри которых вычисляется медиана блока S_k : если $S_k > 0$, бит восстанавливается как 1, иначе – 0 [3]. Такой подход позволяет безошибочно извлечь информацию даже в случае уничтожения или сильного искажения части блоков. Восстановленный одномерный битовый вектор преобразуется в двумерную матрицу, к которой применяется обратное преобразование Арнольда для получения итогового визуального логотипа.

Предложенный метод был подвергнут серии испытаний на устойчивость к различным типам атак с варьируемыми алгоритмическими параметрами. В таблице ниже представлены усредненные значения данных метрик, рассчитанные для каждого отдельного класса атак.

Результаты тестирования метода
Test results of the method

Название атаки	BER	Accuracy	NC	PSNR	SSIM
Шум Гаусса	0.2190	0.7810	0.8626	55.96	0.4549
JPEG	0.0029	0.9971	0.9983	∞	0.9874
Медианный фильтр	0.0127	0.9873	0.9927	67.09	0.9464
Шум соль и перец	0.1035	0.8965	0.9381	58.96	0.6781
Закрашивание	0.0221	0.9779	0.9872	65.93	0.9118

Заключение

В ходе проведенного исследования был разработан и реализован криптостойкий неслепой алгоритм внедрения цифровых водяных знаков, объединяющий преимущества DWT, метода расширения спектра и математического аппарата теории хаоса. Экспериментальное тестирование подтвердило высокую устойчивость предложенной архитектуры.

Список использованных источников / References

1. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8(06), 1259-1284.
2. Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023). A blind and robust color image watermarking scheme based on DCT and DWT domains. Multimedia Tools and Applications, 82(21), 32855-32881.
3. Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020(1), 9597619.

Сведения об авторе

Маутин И.В., магистрант кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mautin.ivan.3@gmail.com.

Information about the author

Mautsin I., Master Student of the Informatics Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, mautin.ivan.3@gmail.com.

УДК 004.056

ФУНКЦИИ ФИЛЬТРАЦИИ И ШИФРОВАНИЯ DNS-СООБЩЕНИЙ НА МЕЖСЕТЕВОМ ЭКРАНЕ CHUWALL

Д.М. Мартинкевич¹, К.О. Яниславский¹, Е.С. Белоусова²

¹Учреждение образования «Национальный детский технопарк»,
г. Минск, Республика Беларусь

²Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе представлено описание реализации функций фильтрации DNS-сообщений и их шифрования для обеспечения информационной безопасности. На основе сервиса BIND9, метода DNS-Sinkholing и списков фильтрации доменов реализована функция проверки DNS-сообщений на межсетевом экране для обнаружения и блокировки кибератак CHUWALL. Для шифрования DNS-сообщений был настроен сервис dnscrypt_proxy, который поддерживает протокол DNS-over-HTTPS. В статье представлены результаты тестирования реализованных функций на межсетевом экране CHUWALL.

Ключевые слова: Межсетевой экран; CHUWALL; DNS; DNS-Sinkholing; BIND9; HaGeZi; TLD-сервер; dnscrypt_proxy; DNS-over-HTTPS (DoH); Яндекс DNS.

FILTERING AND ENCRYPTION FUNCTIONS OF DNS-MESSAGES ON THE CHUWALL FIREWALL

D.M. Martsinkevich¹, K.A. Yanislauski¹, E.S. Belousova²

¹Educational Institution “National Children's Technopark”,
Minsk, Republic of Belarus

²Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus

Abstract. This article describes the implementation of DNS message filtering and encryption functions to ensure information security. Based on the BIND9 service, the DNS-Sinkholing method and domain filtering lists, a function of checking DNS messages has been implemented on the firewall to detect and block the cyber attacks CHUWALL. To encrypt DNS messages, dnscrypt_proxy has been set up, which supports the DNS-over-HTTPS protocol. The article presents the results of testing implemented functions on the CHUWALL firewall.

Keywords: Firewall; CHUWALL; DNS; DNS-Sinkholing; BIND9; HaGeZi; TLD-server; dnscrypt_proxy; DNS-over-HTTPS (DoH); Yandex DNS.

Введение

Протокол DNS по своей архитектуре не предоставляет механизмов обеспечения безопасности. Следовательно, возможны кибератаки типа отравления кэша, DoS, DNS-спуфинг и фишинг [1]. Для обеспечения конфиденциальности и целостности информации существует протокол DNS-over-HTTPS, с помощью которого DNS-трафик инкапсулируется в протокол HTTPS. Целью данной работы является реализация функций фильтрации и шифрования DNS-сообщений путем использования списка фишинговых сайтов, создания корпоративного списка фильтрации и шифрования по протоколу DNS-over-HTTPS (DoH).

Основная часть

В ходе разработки межсетевого экрана для обнаружения и блокировки кибератак CHUWALL [2], работающего на операционной системе Linux Ubuntu Server, реализована функция фильтрации и шифрования DNS-сообщений. Произведено исследование популярных сервисов (Unbound, dnsmasq, BIND9) с открытым исходным кодом для ОС Linux. По результатам сравнения был выбран сервис BIND9 по причине легковесности и эффективности (по сравнению с Unbound), поддержки файлов зон для фильтрации запросов (по сравнению с dnsmasq).

Для фильтрации запросов использован метод DNS-Sinkholing, предназначенный для перенаправления DNS-запросов на заданный сервер. В разрабатываемом межсетевом экране эта функция необходима для предотвращения доступа пользователя к нелегитимным доменам. Список HaGeZi (db.hagezi.rpz) использовался для блокировки фишинговых и рекламных доменов. Также использовался корпоративный список (db.custom.rpz), в который реализована возможность добавления доменов с помощью bash-скрипта.

В соответствии с алгоритмом фильтрации DNS-сообщений (рисунок), если клиент запрашивает нелегитимный домен microsoft.com у локального DNS-сервера BIND9, то проверяется его наличие домена в списках. При обнаружении сервер возвращает вместо реального IP-адреса локальный IP 192.168.50.1, на котором запущен сервис Nginx, возвращающий страницу блокировки доступа при запросе. Подключение клиента к запрашиваемому домену не происходит.

Для легитимных доменов важным остается шифрование DNS-сообщений, ведь такой же сценарий подмены IP-адреса может осуществить нарушитель. Произведено исследование модификаций протокола DNS, а именно DNS-over-HTTPS, DNS-over-TLS, DNSCrypt, DNSSEC. По результатам сравнения был выбран протокол

DNS-over-HTTPS (DoH), так как он работает на порте TCP 443, в отличие от протокола DNS-over-TLS (DoT), работающего на порте TCP 853, что делает его легким для блокировки.

В качестве легковесного DNS-прокси, поддерживающего DoH был выбран сервис `dnsCrypt_proxy`. Для использования TLD-сервера было проведено сравнительный анализ наиболее популярных DNS-провайдеров (Google DNS, Яндекс DNS, Белтелеком). В результате было решено использовать Яндекс DNS по причине нахождения серверов на территории Союзного государства и наличия большого количества кириллических доменов.



Алгоритм фильтрации DNS-сообщений для нелегитимного домена
DNS-messages filtration algorithm for illegitimate domain

Произведена проверка работы протокола DNS-over-HTTPS, при которой в дампе трафика не должны быть обнаружены сетевые пакеты с содержанием протокола DNS на седьмом уровне модели OSI. Соответственно должны быть обращения к IP-адресу TLD-сервера Яндекс DNS Safe по протоколу TLS на порт 443.

Заключение

Таким образом, было установлено, что реализация DNS-сервера на основе BIND9 и метода DNS-Sinkholing с использованием списка HaGeZi и корпоративного списка позволяет обеспечить фильтрацию DNS-сообщений, тем самым предотвратив коммуникацию пользователя с потенциально вредоносным доменом. Также установлено, что для шифрования DNS-сообщений лучше всего подходит протокол DNS-over-HTTPS (DoH), используемый сервисом `dnsCrypt_proxy` для обращения к TLD-серверу. Полученные результаты позволяют рекомендовать межсетевой экран CHUWALL для блокировки попыток

обращения к вредоносным доменам, что может повысить уровень информационной безопасности различных организаций.

Список использованных источников

1. Борботько Ф.Т. (2023) Атаки с использованием DNS протокола и противодействие им. *Технические средства защиты информации*. 22–23.
2. Белоусова Е.С., Мальцев В.Л., Мартинкевич Д.М., Яниславский К.О. (2026) Маршрутизатор с функциями анализа сетевого трафика. *Будущее через исследования*. 52–57.

References

1. Borbotko F.T. (2023) Attacks using the DNS protocol and counteracting it. *Technical means of information protection*. 22-23.
2. Belousova E.S., Maltsev V.L., Martsinkevich D.M., Yanislauski K.O. (2026) Router with network traffic analysis functions. *The future through research*. 52-57.

Сведения об авторах

Мартинкевич Д.М., учащийся, учреждение образования «Национальный детский Технопарк», srilankainform@gmail.com.

Яниславский К.О., учащийся, учреждение образования «Национальный детский Технопарк», kirill.uspech@gmail.com.

Белоусова Е.С. канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Martsinkevich D., Student, Educational Institution “National Children's Technopark”, srilankainform@gmail.com.

Yanislauski K., Student, Educational Institution “National Children's Technopark”, kirill.uspech@gmail.com.

Belousova E., PhD, Associate Professor, Information Protection Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, belousova@bsuir.by.

УДК 004.056:336.71(076)

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ИЗМЕНЕНИЯ СОСТАВА

А.М. Тимофеев¹, Д.В. Шляхтун², Ли Чэнтинъюй¹, Хуан Цзыхань¹

¹Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

²Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь

Аннотация. Разработана процедура обезличивания персональных данных, основанная на базе метода изменения состава. Данная процедура позволяет обезличивать

персональные данные буквенного и числового типов, не требует использования больших вычислительных ресурсов для оборудования легитимных пользователей и обеспечивает достаточно высокий уровень информационной безопасности за счет изменения статистических свойств полученных обезличенных персональных данных, в сравнении с исходными персональными данными.

Ключевые слова: информационные системы; персональные данные; защита информации; обезличивание персональных данных; методы обезличивания персональных данных; метод изменения состава.

DEPERSONALIZATION OF PERSONAL DATA BASED ON THE METHOD OF CHANGING THE COMPOSITION

A.M. Timofeev¹, D.V. Shliakhtun², Chengtingyu Li¹, Huang Zihan¹

¹*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

²*Educational Institution "National Children's Technopark",
Minsk, Republic of Belarus*

Abstract. The procedure for depersonalization of personal data, based on the composition change method, was developed. This procedure allows for the depersonalization of personal data of the letter and numeric types, does not require the use of large computing resources for the equipment of legitimate users and ensures a sufficiently high level of information security by changing the statistical properties of the received depersonalized personal data in comparison with the original personal data.

Keywords: information systems; personal data; information protection; depersonalization of personal data; methods of depersonalization of personal data; method of changing the composition.

Введение

В настоящее время в большинстве существующих информационных систем обрабатываются персональные данные [1–3]. Под персональными данными будем понимать любую информацию о физическом лице, посредством которой физическое лицо либо идентифицировано, либо может быть идентифицировано.

К числу персональных данных относят, например, физиологические и биологические особенности человека, наследуемые и приобретенные генетические характеристики, а также информацию, касающуюся его национальной, расовой принадлежности, членства в профессиональных союзах и прочие [1–3]. Важно отметить, что в Республике Беларусь информационная безопасность систем, в которых обрабатываются персональные данные, может быть обеспечена посредством обезличивания персональных данных. Обезличиванием персональных данных называют любое действие или совокупность действий, совершаемых с персональными данными, в результате которых становится невозможным определение их принадлежности субъекту персональных данных без дополнительной информации.

В соответствии с требованиями законодательства Республики Беларусь в сфере защиты персональных данных одним из методов обеспечения их информационной безопасности является метод изменения состава. Сущность этого метода заключается в следующем. Часть персональных данных, подлежащих обезличиванию, удаляют, другую часть изменяют, а оставшуюся часть преобразуют таким образом, что изменяется семантическое представление данных. В случае удаления персональных данных или изменения их отдельных частей требуется отдельно хранить информацию о том, какие именно данные удалены и изменены. В противном случае становится невозможным выполнение процедуры деобезличивания.

Деобезличивание – это процесс, в результате которого обезличенные персональные данные принимают исходный вид.

Важно отметить, что существующие реализации метода изменения состава характеризуются достаточно низким уровнем информационной безопасности, поскольку в случае изменения семантического представления данных статистические свойства обезличенных данных остаются такими же, как и для естественного языка. В связи с этим целью данной работы являлась разработка структурной схемы, позволяющей реализовывать обезличивание персональных данных на основе метода изменения состава, которая свободна от недостатков существующих схем обезличивания персональных данных.

Объектом исследования являлся метод изменения состава, применяемый для обезличивания персональных данных в соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации.

Предметом исследования являлось установление процедуры обезличивания персональных данных, в результате реализации которой обеспечивается повышение уровня их информационной безопасности за счет изменения статистических свойств, в сравнении с исходными персональными данными.

Реализация процедуры обезличивания персональных данных

Процедура обезличивания персональных данных реализована программно и заключается в следующем. Исходные персональные данные, подлежащие обезличиванию, подают на блок загрузки персональных данных, в котором выделяются атрибуты персональных данных, подлежащих обезличиванию. Затем исходные персональные данные поступают на блок фрагментации, где персональные данные разделяют на 64-битные части. После этого осуществляют итерационный процесс обезличивания, в который входит использование 64-битного вектора инициализации, значение которого для каждого текущего блока инкрементируют, а также процедура генерации раундовых секретных

ключей и операции сложения по модулю 2^{32} , нелинейной подстановки, согласно секретной таблице замены, и циклического сдвига влево на 11 разрядов согласно ГОСТ 28147-89. После выполнения всех 32 циклов итерационного процесса полученные блоки конкатенируют и формируют обезличенные персональные данные. Первичный анализ обезличенных персональных данных показал, что статистические свойства этих данных изменились, в сравнении со статистическими свойствами исходных персональных данных. В связи с этим авторам настоящей работы видится перспективным проведение исследований, направленных на оценку достигнутого уровня информационной безопасности персональных данных, что планируется выполнить в дальнейшем.

Заключение

При реализации обезличивания персональных данных буквенного и числового типов достаточно важным является осуществление процедуры обезличивания таким образом, чтобы статистические свойства обезличенных персональных данных не совпадали со статистическими свойствами исходных персональных данных, что повышает достигаемый уровень информационной безопасности. Предложена процедура обезличивания персональных данных буквенного типа на основе метода изменения состава, использование которой позволяет достичь эффекта, при котором статистические свойства исходных персональных данных отличаются от статистических свойств, обезличенных персональных данных. Данная процедура не требует наличия больших вычислительных ресурсов, что расширяет область ее возможного практического применения.

Список использованных источников

1. Ворона, В. А. (2023) *Биометрическая идентификация личности*. Москва, Горячая линия-Телеком.
2. Коллинз, М. (2020) *Защита сетей. Подход на основе анализа данных*. Москва, ДМК Пресс.
3. Остапенко, Г. А. (2020) *Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия*. Москва, Горячая линия-Телеком.

References

1. Vorona V. A. (2023) *Biometric Identification of Personality*. Moscow, Goryachaya Liniya-Telecom (in Russian).
2. Collins M. (2020) *A Data-Based Approach*. Moscow, DMK Press (in Russian).
3. Ostapenko G. A. (2020) *Information Operations and Attacks in Socio-Technical Systems: Organizational and Legal Aspects of Counteraction*. Moscow, DMK Press (in Russian).

Сведения об авторах

Тимофеев А.М., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», tambsuir@bsuir.by.

Шляхтун Д.В., учащаяся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», rd2859002@gmail.com.

Ли Ч., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lcaomi@outlook.com.

Хуан Ц., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», 1913017013@qq.com.

Information about the authors

Timofeev A., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", tambsuir@bsuir.by.

Shliakhtun D., Student of the direction "Information Security", Educational Institution "National Children's Technopark", rd2859002@gmail.com.

Chengtingyu Li, Master's Student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lcaomi@outlook.com.

Huang Z., Master's Student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", 1913017013@qq.com.

УДК 537.87:539.216

МНОГОСЛОЙНЫЕ ТОНКОПЛЕНОЧНЫЕ ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С РАЗВИТЫМ ПЕРИОДИЧЕСКИМ РЕЛЬЕФОМ ПОВЕРХНОСТИ

А.Д. Гладинов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Приведены результаты исследований взаимодействия электромагнитного излучения (ЭМИ) СВЧ-диапазона (2,0–17,0 ГГц) с многослойными тонкопленочными экранами, имеющими развитый периодический рельеф поверхности. Показано, что экраны с нанесенными на полимерные подложки покрытиями систем Al-(Fe-Ni) и Al-Cu-(Fe-Ni) характеризуются значениями коэффициента передачи электромагнитного излучения в пределах от –8,2 до –41,0 дБ. Данные экраны перспективны для защиты электронных устройств от воздействия электромагнитного излучения СВЧ-диапазона.

Ключевые слова: тонкопленочные экраны; многослойное покрытие; периодический рельеф; электронно-лучевое испарение; покрытия систем Al-(Fe-Ni) и Al-Cu-(Fe-Ni).

MULTILAYER THIN-FILM ELECTROMAGNETIC RADIATION SHIELDS WITH A DEVELOPED PERIODIC SURFACE RELIEF

A.D. Gladinov

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article presents the results of the study of microwave radiation (2.0–17.0 GHz) interaction with multilayer thin-film shields with a developed periodic surface relief. It is shown that shields with Al-(Fe-Ni) and Al-Cu-(Fe-Ni) coatings applied to polymer substrates are characterized by electromagnetic radiation transmission coefficients ranging from –8.2 to –41.0 dB. These shields are promising for protecting electronic devices from microwave radiation.

Keywords: thin-film shields; multilayer coating; periodic relief; electron beam evaporation; coatings of the Al-(Fe-Ni) and Al-Cu-(Fe-Ni) systems.

Введение

Известно, что искусственно созданные периодические структуры, в частности, двумерные метаповерхности, имеют уникальные свойства пропускания и отражения электромагнитного излучения (ЭМИ), обусловленные, преимущественно, поверхностным электромагнитным импедансом [1]. Достижения в области метаматериалов и метаповерхностей открывают новые возможности для создания материалов с управляемыми свойствами, которые не проявляются природными материалами [2, 3].

Свойства метаматериалов и метаповерхностей определяются повторяющейся периодической формой, геометрией и ориентацией структур, образующих метаматериал. Это позволяет сформировать структурированные среды и поверхности со свойствами, которые не встречаются в естественных материалах, и применять полученные метаматериалы и метаповерхности для управления ЭМИ оптического, СВЧ и терагерцового диапазонов длин волн. При размерах периодических структур меньших характерной длины волны излучения они позволяют сформировать необходимые защитные свойства за счет дифракции и интерференции излучения. При этом характерный размер периодических структур для микроволнового излучения составляет единицы миллиметров. Типичные метаматериалы и метаповерхности СВЧ-диапазона формируются из периодически повторяющихся электропроводящих элементов в диэлектрическом материале или в многослойных металлодиэлектрических системах.

Основная часть

Тонкопленочные покрытия наносили методом электронно-лучевого испарения с помощью модернизированной установки вакуумного

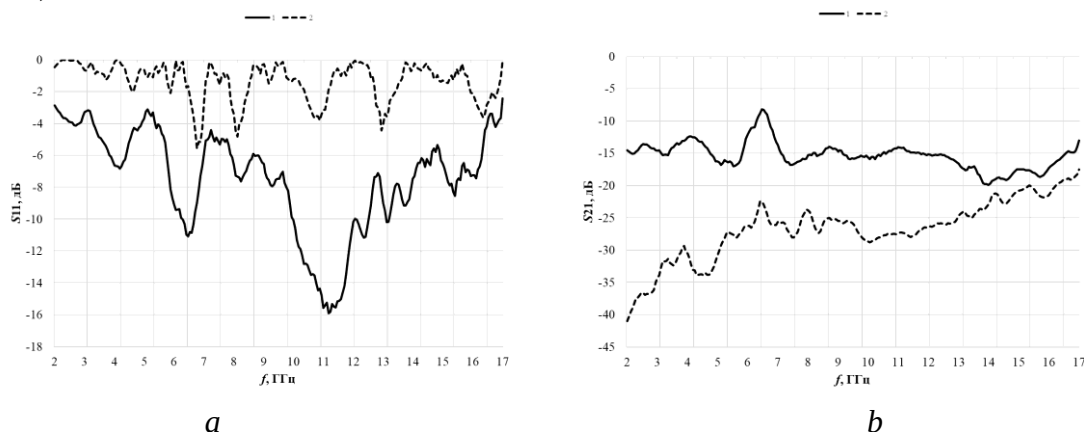
напыления ВУ-1А. Покрyтия наносили на полимерную подложку из поликарбоната размерами $300 \times 300 \times 0,5$ мм имеющую периодический рельеф, состоящий из полусфер диаметром 16 мм, имеющих высоту 8 мм, расположенных рядами 17×17 шт. Выбор данного диаметра сфер связан с обеспечением наилучшего экранирования ЭМИ в верхнем диапазоне частот, так как с увеличением частоты эффективность экранирования снижается. Известно, что длина волны L при частоте 18 ГГц составляет 16,7 мм, и для обеспечения эффективного экранирования на данных частотах оптимальными являются полусферы диаметром $D \approx 16$ мм, т.е. при соотношении $L:D \approx 1:1$. Кроме того, использование поверхностно-развитой подложки позволяет увеличить площадь поверхности экрана на 64 % в сравнении с таким же по размерам плоским экраном, что также повышает защитные свойства. В качестве покрытий использовали системы, состоящие из токопроводящих и магнитных слоев. Для нанесения токопроводящих слоев использовали медь марки М0 и алюминий марки А₅N, для магнитного слоя использовали сплав железо-никель азеотропного состава Fe₅₆Ni₄₄ [4].

В соответствии с отработанными методиками, представленными в работе [5], были нанесены покрытия со слоями Al, Cu и Fe-Ni толщинами 150 нм каждый. Системы покрытий Al-(Fe-Ni) и Al-Cu-(Fe-Ni) имели общую толщину 300 и 450 нм соответственно. Исследование коэффициентов отражения и передачи проводили, используя измерительный модуль SNA 0.01–18. Измерения с применением этого модуля проводили в диапазоне частот 2–17 ГГц в соответствии с ГОСТ 20271.1–91 «Изделия электронные СВЧ. Методы измерения электрических параметров».

Частотные зависимости коэффициента отражения (S_{11}) и передачи (S_{21}) экранов с покрытиями систем Al-(Fe-Ni) и Al-Cu-(Fe-Ni) представлены на рисунке. Значения коэффициента отражения ЭМИ в диапазоне частот 2–17 ГГц экранов, изготовленных на основе покрытий системы Al-(Fe-Ni) (часть *a* рисунка, кривая 1) изменяются в пределах от (–2,4) до (–15,8) дБ. Значения S_{11} экранов с нанесенным на подложку дополнительным токопроводящим слоем Cu системы Al-Cu-(Fe-Ni) (часть *a* рисунка, кривая 2) увеличиваются во всем исследованном диапазоне частот ЭМИ и изменяются в пределах от (–0,1) до (–5,6) дБ.

Значения коэффициента передачи ЭМИ в диапазоне частот 2–17 ГГц для экранов системы Al-(Fe-Ni) (часть *b* рисунка, кривая 1) изменяется в пределах от (–19,9) до (–8,2) дБ, для системы Al-Cu-(Fe-Ni) (часть *b* рисунка, кривая 2) от (–41,0) до (–17,4) дБ. Как видно из полученных результатов исследований значений S_{11} и S_{21} добавление подслоя Cu толщиной 150 нм приводит к увеличению значений коэффициента отражения ЭМИ более чем в 2,5 раза, по сравнению с экраном ЭМИ без него. При этом за счет увеличения отражения ЭМИ

возрастает коэффициент передачи до 2 раз по сравнению с системой Al-(Fe-Ni).



a **b**
Частотные зависимости в диапазоне частот 2–17 ГГц покрытий систем
Al-(Fe-Ni) (кривая 1) и Al-Cu-(Fe-Ni) (2): *a* – S_{11} ; *b* – S_{21}
Frequency dependences in the frequency range of 2-17 GHz of system coatings
Al-(Fe-Ni) (curve 1) and Al-Cu-(Fe-Ni) (2): *a* – S_{11} ; *b* – S_{21}

Заключение

Установлено, что значения коэффициента отражения S_{11} ЭМИ в диапазоне частот 2–17 ГГц экранов с нанесенными на полимерную подложку, имеющую периодический рельеф поверхности, покрытиями систем Al-(Fe-Ni) и Al-Cu-(Fe-Ni), изменяются в следующих пределах: (–2,4)–(–15,8) дБ и (–0,1)–(–5,6) дБ соответственно. Коэффициент передачи данных экранов изменяется в следующих пределах: (–19,9)–(–8,2) дБ и (–41,0)–(–17,4) дБ соответственно.

Экран с покрытием системы Al-Cu-(Fe-Ni) имеет повышенные значения коэффициента отражения до 2,5 раз и коэффициента передачи до 2 раз.

Список использованных источников

1. Xu, Z. Surface Waves on Equivalent Impedance Metasurfaces: Recent Developments and New Goals / Z. Xu // 2024 Photonics & Electromagnetics Research Symposium (PIERS), Chengdu, China, 21–25 April 2024. — IEEE, 2024. — P. 1–7. — doi: 10.1109/PIERS62282.2024.10618400
2. Метаповерхность на основе одновитковых планарных спиралей со свойством не отражающего поглотителя в СВЧ диапазоне / И. А. Фаняев, А. Л. Самофалов, И. В. Семченко [и др.] // Проблемы физики, математики и техники. – 2024. – № 3 (60). – С. 38–43.
3. Максимова, А. Г. Широкополосная поглощающая метаповерхность на основе воды / А. Г. Максимова, М. А. Одит // Матер. VIII Всероссийской научно-технической конференции «Электроника и микроэлектроника СВЧ». – Санкт-Петербург, 3–6 июня 2019 г. – С. 514–518.

4. Gladinov, A. D. S-Parameters of Flexible Electromagnetic Radiation Shields with Fe–Ni System Coating / A. D. Gladinov, O. V. Boiprav, V. A. Bogush // Materials Physics and Mechanics. 2024. Vol. 52, Iss. 5. P. 74–82.

5. Гладинов, А. Д. Характеристики отражения и передачи многослойных тонкопленочных экранов электромагнитного излучения в СВЧ-диапазоне / А. Д. Гладинов, О. В. Бойправ, В. А. Богуш // Доклады БГУИР. 2025. Т. 23, № 6. С. 56–64.

References

1. Xu, Z. Surface Waves on Equivalent Impedance Metasurfaces: Recent Developments and New Goals / Z. Xu // 2024 Photonics & Electromagnetics Research Symposium (PIERS), Chengdu, China, 21–25 April 2024. IEEE, 2024. P. 1–7. doi: 10.1109/PIERS62282.2024.10618400.

2. Metasurface Based on Single-Turn Planar Spirals with the Property of a Non-Reflective Absorber in the Microwave Range / I. A. Fanyayev, A. L. Samofalov, I. V. Semchenko [et al.] // Problems of Physics, Mathematics and Technology. 2024. No. 3 (60). P. 38–43 (in Russian).

3. Maksimova, A. G. Broadband Absorbing Metasurface Based on Water / A. G. Maksimova, M. A. Odit // Proceedings of the VIII All-Russian Scientific and Technical Conference “Microwave Electronics and Microelectronics”. St. Petersburg, June 3–6, 2019. P. 514–518 (in Russian).

4. Gladinov, A. D. S-Parameters of Flexible Electromagnetic Radiation Shields with Fe–Ni System Coating / A. D. Gladinov, O. V. Boiprav, V. A. Bogush // Materials Physics and Mechanics. 2024. Vol. 52, Iss. 5. P. 74–82.

5. Gladinov A. D., Boiprav O. V., Bogush V. A. Reflection and Transmission Characteristics of Multilayer Thin-Film Screens of Electromagnetic Radiation in the Microwave Range / A. D. Gladinov, O. V. Boiprav, V. A. Bogush // Doklady BGUIR. 2025. Vol. 23, iss. 6. P. 56–64 (in Russian).

Сведения об авторе

Гладинов А. Д., асп. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.gladinov@bsuir.by.

Information about the author

Gladinov A. D., Postgraduate at Information Protection Department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.gladinov@bsuir.by.

УДК 004.056

АППАРАТНО-ПРОГРАММНЫЕ МЕХАНИЗМЫ БЛОКИРОВКИ ВРЕДОНОСНОГО КОДА

А.К. Крамаренко, А.В. Лопато

*Учреждение образования «Брестский государственный технический
университет», г. Брест, Республика Беларусь*

Аннотация. Рассмотрены аппаратные решения на уровне процессора (NX/XD-бит, технологии изолированных сред исполнения), программные методы контроля приложений (AppLocker, Windows Defender Application Control) и интеллектуальные системы на базе репутационного анализа (Smart App Control). Также приводятся сведения о поведенческих методах обнаружения аномалий выполнения программ и динамических песочницах.

Ключевые слова: NX/XD-бит; контроль приложений; Smart App Control; доверенная среда исполнения; поведенческий анализ; динамическая песочница.

HARDWARE-SOFTWARE MECHANISMS FOR MALICIOUS CODE BLOCKING

A.K. Kramarenko, A.V. Lopato

*Educational Institution "Brest State Technical University",
Brest, Republic of Belarus*

Abstract. Hardware solutions at the processor level (NX/XD-bit, isolated execution environment technologies), software application control methods (AppLocker, Windows Defender Application Control) and intelligent systems based on reputation analysis (Smart App Control) are considered. Also provides information about behavioral methods for detecting program execution anomalies and dynamic sandboxes.

Keywords: NX/XD-bit; application control; Smart App Control; trusted execution environment; behavioral analysis; dynamic sandboxing.

Введение

В настоящее время угрозы кибербезопасности видоизменяются, а применяемые сигнатурные методы защиты от вредоносного кода реагируют на них с задержкой. Они зачастую не своевременно реагируют на полиморфные вредоносные программы [1]. Это требует смещения применяемой защиты в сторону проактивного блокирования такой активности. В данной статье будут приведены результаты исследования некоторых аппаратно-программных комплексов защиты информации, а именно – механизмы блокировки выполнения вредоносного кода. Цель – исследование аппаратно-программных методов блокировки вредоносного кода и оценка перспективных направлений.

Основная часть

Блокировка вредоносного кода отличается от его обнаружения и лечения. Реактивные методы разрешают кратковременное выполнение

вредоносного кода до момента его обнаружения, а проактивная блокировка – предотвращение факта запуска или исполнения деструктивных инструкций. Концепция защиты строится на многоуровневом подходе (Defense in Depth) с аппаратной «песочницей» на уровне ядра. В тоже время программные надстройки управляют политиками запуска. Ключевое изменение в защите – переход от подхода «разрешено все, что не запрещено» к подходу «запрещено все, что не разрешено» [2]. В таблице представлены результаты сравнения реактивного и проактивного подходов к защите.

Сравнение реактивного и проактивного подходов к защите
Comparison of reactive and proactive approaches to protection

Характеристика	Реактивный подход (сигнатурный)	Проактивный подход (блокирование)
Принцип работы	Поиск совпадений с базой угроз	Предотвращение выполнения неизвестного кода
Время реакции	После появления сигнатуры	До запуска кода
Защита от новых угроз	Отсутствует до обновления баз	Высокая (поведенческий анализ)
Нагрузка на систему	Высокая (постоянное сканирование)	Средняя (проверка при запуске)
Ложные срабатывания	Низкие	Выше, но компенсируются настройками

Аппаратные механизмы выполняются на уровне центрального процессора. Один из основных аппаратных механизмов – это бит запрета исполнения. Он реализован в процессорах Intel (как Execute Disable Bit) и в AMD (как Enhanced Virus Protection). Суть заключается в аппаратной поддержке страничной организации памяти. Это является важным для отражения классических атак типа переполнения буфера. В случае если процессор пытается выполнить команду из области с флагом «No eXecute», он генерирует соответствующее исключение. Далее операционная система этот завершает процесс [3].

В современных операционных системах (Windows, Linux, др.) этот механизм используется совместно с программной реализацией Data Execution Prevention. Такая реализация закрывает целый класс уязвимостей, связанных с выполнением кода в неположенных сегментах памяти. Программные механизмы часто надстраиваются над аппаратными для обеспечения логики принятия решений о доверии к исполняемому коду (Control Flow Integrity или целостность потока управления). Согласно базе знаний MITRE ATT&CK, одна из эффективных контрмер – предотвращение выполнения кода через контроль приложений и блокировку скриптов. Инструменты (AppLocker, Windows Defender

Application Control, др.) разрешают администраторам задавать политики, разрешающие запуск тех исполняемых файлов, которые имеют доверенную цифровую подпись или же хранятся в определенных защищенных путях. Так блокируется выполнение «живущих с земли» бинарных файлов и скриптов [3].

Также новый виток развития – системы на базе репутационного анализа. Windows 11 Smart App Control изменяет существующую логику работы антивирусной программы. Перед запуском файла SAC обращается к облачной службе репутации Microsoft и анализирует цифровую подпись, также применяет модели машинного обучения. Если репутация файла неизвестна или он признается вредоносным, его запуск блокируется. Это решение работает проактивно.

Атаки часто направлены не на исполняемые файлы, а на скрипты (JavaScript, VBA, др.), также на цепочки поставок программного обеспечения. Патент US 9648032 описывает метод блокировки скриптов. Он основан на перехвате запроса к серверу. В области безопасной разработки появился и класс решений – Dependency Firewall (межсетевой экран для зависимостей), который изучает открытые компоненты и библиотеки до того, как они попадут в код. Это решение в реальном времени блокирует уязвимые артефакты.

Заключение

Подводя итог, отметим, что аппаратный уровень создает базу, путем разделения памяти на исполняемые и неисполняемые области и, тем самым, препятствует базовым классам атак. Программный уровень управления использует политику «белых списков» и репутационного анализа. На этом уровне запрещается запуск неподписанного или малоизвестного кода. Перспективные же методы (анализ аномалий выполнения, др.) ориентированы на блокировку неизвестных угроз и атак нулевого дня. И, совместное использование всех этих механизмов повышает степень защиты, минимизируя временной промежуток между появлением угрозы и ее блокировкой.

Список использованных источников

1. Крамаренко А. К., Русенко В. Н. (2024) Интеграция программного обеспечения в бизнес: процесс, проблемы и перспективы. Интеллектуальные ресурсы – региональному развитию. (1), 232–237.
2. Косолапов Ю. В., Павлова Т. А. (2024) Об исследовании одного способа выявления аномального выполнения программы. Моделирование и анализ информационных систем. 31 (2), 152–163.
3. Иванов М. А., Чугунков А. А. (2024) Криптографические методы защиты информации. 3-е изд., испр. и доп. Москва: Юрайт. 315 с.

References

1. Kramarenko A. K., Rusenko V. N. (2024) Integration of Software into Business: Process, Problems and Prospects. Intellectual Resources – Regional Development. (1), 232–237 (in Russian).
2. Kosolapov Yu. V., Pavlova T. A. (2024) On the Study of a Method for Detecting Anomalous Program Execution. Modeling and Analysis of Information Systems. 31 (2), 152–163 (in Russian).
3. Ivanov M. A., Chugunkov A. A. (2024) Cryptographic Methods of Information Protection. 3rd ed., corrected and supplemented. Moscow: Yurayt. 315 p. (in Russian).

Сведения об авторах

Крамаренко А.К., канд. экон. наук, доц., доц. кафедры бухгалтерского учета, анализа и аудита, учреждение образования «Брестский государственный технический университет», annnakramarenko@yandex.by.

Лопато А.В., студент факультета электронно-информационных систем, учреждение образования «Брестский государственный технический университет», artemlopato11@gmail.com.

Information about the authors

Kramarenko A.K., Cand. Sci. (Econ.), Associate Professor, Associate Professor of the Department of Accounting, Analysis, and Audit, Educational Institution “Brest State Technical University”, annnakramarenko@yandex.by

Lopato A.V., student, Faculty of Electronic Information Systems, Educational Institution “Brest State Technical University”, artemlopato11@gmail.com.

UDC 004.056

ENHANCING CYBERSECURITY RESILIENCE THROUGH AN INTEGRATED ARTIFICIAL INTELLIGENCE FRAMEWORK

H.H. Sudani

Scientific Research Commission, Baghdad, Iraq

Abstract. As cyber threats become increasingly complex, artificial intelligence (AI) has become a critical tool for strengthening cybersecurity systems. This article examines how AI improves the effectiveness of cyber defense through real-time threat detection, behavioral analysis, and automated response mechanisms. However, the integration of AI also creates new vulnerabilities, including adversarial attacks, data dependency risks, and ethical concerns related to surveillance and privacy. The dual nature of AI – as a powerful defense mechanism and a potential security risk – underscores the need for responsible implementation. The paper concludes by emphasizing the importance of transparency, robust data governance, and continuous model evaluation in building resilient AI-powered cybersecurity frameworks.

Keywords: artificial intelligence; cybersecurity; threat detection; adversarial attacks; data privacy; security automation.

Introduction

Artificial Intelligence (AI) is revolutionizing cybersecurity by enhancing threat detection, risk assessment, and automated response. AI refers to machines simulating human intelligence through learning and decision-making [1]. According to [2] AI-driven tools analyze vast datasets in real-time, identifying threats with greater accuracy, unlike traditional security systems.

AI plays a critical role in cybersecurity, offering powerful defensive capabilities while also posing significant security risks. As a defense tool, AI enhances threat detection, automates response mechanisms, and improves security efficiency. AI-powered systems can analyze vast amounts of data in real time, identify patterns, and detect anomalies indicative of cyber threats [2]. Machine learning models, for example, are used in intrusion detection systems (IDS) to differentiate between normal and malicious network activities [3].

AI in cybersecurity is essential for combating evolving cyber threats, but it must be implemented with caution to mitigate potential risks [4].

Main Part

Despite AI's potential in aiding cybersecurity, AI presents several challenges that organizations must address. Two major concerns to be addressed are categorized to include adversarial attacks and data privacy risks.

1. Adversarial Attacks. While AI enhances cybersecurity, it is also vulnerable to adversarial attacks, where cybercriminals manipulate AI models to bypass security systems. Attackers use techniques such as data poisoning, where malicious data is fed into AI systems to corrupt their learning process, leading to false predictions or security blind spots. Allowing threats to go undetected [5]. Adversarial attacks raise concerns about AI's reliability in critical security applications.

2. Data Privacy Risks. AI-driven cybersecurity systems rely on vast amounts of data, often including sensitive personal or corporate information. Improper data handling or inadequate security measures can lead to data breaches, unauthorized access, or misuse.

3. Bias and False Positives in AI Models. Bias and false positives in AI models pose significant challenges in cybersecurity, as flawed training data and detection errors can lead to inaccurate threat assessments and security vulnerabilities.

The increasing complexity and frequency of cyber threats have necessitated the integration of Artificial Intelligence (AI) in cybersecurity [6].

AI offers advanced capabilities for threat detection, incident response, and risk mitigation through machine learning, automation, and predictive analytics.

1. AI-powered threat Detection and Anomaly Identification. Traditional cybersecurity systems rely heavily on signature-based detection, which is ineffective against novel threats. AI-driven threat detection utilizes machine learning (ML) and deep learning to analyze large datasets, recognize patterns, and detect anomalies in real time [3]. Anomaly-based detection leverages AI to differentiate between normal and abnormal system behavior, identifying potential cyberattacks such as zero-day exploits and advanced persistent threats (APTs).

2. Automated Incident Response and Mitigation. AI enhances cybersecurity by automating incident response, reducing the time required to mitigate threats. Security Orchestration, Automation, and Response (SOAR) systems integrate AI to analyze security incidents and execute predefined response actions without human intervention. For example, AI-powered intrusion detection systems (IDS) and intrusion prevention systems (IPS) can automatically block malicious traffic, isolate compromised systems, and apply security patches in real time.

3. AI vs. Traditional Cybersecurity Effectiveness Cybersecurity has evolved significantly with the introduction of Artificial Intelligence (AI), which enhances threat detection, response, and prevention mechanisms. A comparison between AI-powered cybersecurity and traditional cybersecurity shown in the table 1 on a scale of 10 points score.

This table below provides a clear comparison of how AI improves cybersecurity effectiveness in terms of speed, accuracy, adaptability, and proactive defense strategies.

Future trends of artificial intelligence in cybersecurity are following.

1. The Zero Trust Security Model and AI's Role the Zero Trust Security Model operates on the principle of "never trust, always verify," requiring continuous authentication for all users and devices, regardless of their location. AI is crucial in implementing Zero Trust by continuously monitoring user behavior and network activity.

2. AI-Driven Identity Verification for Enhanced Authentication AI is enhancing identity verification methods to strengthen authentication processes. Traditional methods like passwords are vulnerable to breaches, but AI offers more secure alternatives, such as biometric recognition (e.g., facial recognition, voice biometrics, and behavioral biometrics).

3. Ethical and Regulatory Frameworks for AI Cybersecurity With the increasing use of AI in cybersecurity, ethical concerns and regulatory frameworks are essential. AI systems must be designed to ensure fairness,

transparency, and accountability to avoid bias and misuse. For example, AI could unintentionally discriminate against certain groups or lead to issues of privacy invasion when analyzing personal data.

A comparison between AI-powered cybersecurity and traditional cybersecurity

Security Metric	Traditional Cybersecurity	AI-Powered Cybersecurity
Detection Speed	Score: 5 – Relies on signature-based detection, slower in identifying new threats.	Score: 9 – Uses real-time anomaly detection and machine learning for faster identification.
Accuracy	Score: 6 – Prone to false positives and false negatives, less effective at identifying novel threats.	Score: 9 – Learns from historical data, improving accuracy and reducing false positives/negatives.
Response Time	Score: 5 – Requires manual intervention, causing delays in mitigation.	Score: 9 – Automates incident response, instantly neutralizing threats.
Adaptability	Score: 4 – Struggles with new, evolving attack methods; dependent on signature updates.	Score: 8 – Continuously learns and adapts to new cyber threats through machine learning.
Threat Prediction	Score: 3 – Reactive, identifies threats only after they occur.	Score: 9 – Uses predictive analytics to foresee potential attacks and take proactive measures.

Conclusion

In conclusion, artificial intelligence (AI) is reshaping the cybersecurity landscape by enabling real-time threat detection, driving innovations such as zero-trust security and AI-powered identity verification, and preparing defenses against future challenges like quantum computing. While its capabilities make it a powerful tool for digital security, the potential for AI misuse by cybercriminals, along with risks such as bias, privacy violations, and false alarms, underscores the need for strong ethical standards, regulatory oversight, and continuous improvement. With responsible deployment and sound governance, AI can significantly enhance cybersecurity, making digital systems more secure, resilient, and adaptable to emerging threats.

References

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
2. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2022). AI-driven cybersecurity: Threat intelligence and risk mitigation. *Cybersecurity and AI Journal*, 8(1), 20-35.
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176.
4. Liu, Z., Chen, Y., & Zhang, H. (2022). Quantum-Resistant Cryptography and AI: A Survey. *IEEE Access*, 10, 6501-6514.

5. Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2017). Practical Black-Box Attacks Against Machine Learning. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 506-519.

6. Н.Н. Судани. Artificial Intelligence Securing In Cyberspace // XXIII International Scientific And Technical Conference "Technical Means Of Information Protection", April 08, 2025, Minsk. Minsk: BSUIR, 2025. - p. 32-34.

Information about the author

Sudani H., Dr.Sci.(Eng, Head of the Department, Ministry of Higher Education and Scientific Research. hayder.h.kareem@src.edu.iq.

УДК 004.056:378.016

АДАПТАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОД ТРЕБОВАНИЯ СТЕКА ОТЕЧЕСТВЕННЫХ ОС (НА ПРИМЕРЕ ASTRA LINUX)

А.И. Бердник

ООО «Альпиндустрия», г. Минск, Республика Беларусь

Аннотация. Переход государственных структур на доверенные программные решения, включая Astra Linux Special Edition, требует пересмотра подходов к обучению специалистов по информационной безопасности. В работе проанализированы противоречия между актуальными запросами работодателей и содержанием классических образовательных программ. Рассмотрены ключевые архитектурные особенности отечественной платформы, в частности механизмы мандатного управления доступом на базе встроенной подсистемы PARSEC. Предложены практические пути трансформации лабораторных практикумов для эффективного формирования профильных компетенций и сокращения периода адаптации молодых специалистов.

Ключевые слова: импортозамещение; Astra Linux; образовательные программы; информационная безопасность; мандатное управление доступом; компетентностный разрыв; подсистема PARSEC; технологический суверенитет; лабораторный практикум; подготовка кадров.

ADAPTATION OF INFORMATION SECURITY EDUCATIONAL PROGRAMS TO THE REQUIREMENTS OF DOMESTIC OS STACK (ON THE EXAMPLE OF ASTRA LINUX)

A.I. Berdnik

Alpindustria LLC, Minsk, Republic of Belarus

Abstract. The transition of state structures to trusted software solutions, including Astra Linux Special Edition, requires a revision of approaches to training information security specialists. The paper analyzes the contradictions between the current needs of employers and the content of classical educational programs. The key architectural features of the domestic platform are considered, in particular, the mandatory access control mechanisms based on the built-in PARSEC subsystem. Practical ways of transforming laboratory workshops to effectively form specialized competencies and reduce the adaptation period of young specialists are proposed.

Keywords: import substitution; Astra Linux; educational programs; information security; mandatory access control; competence gap; PARSEC subsystem; technological sovereignty; laboratory workshop; personnel training.

Введение

Стратегия цифрового развития и курс на технологический суверенитет диктуют необходимость перевода критически важной ИТ-инфраструктуры на доверенное программное обеспечение. Одной из базовых платформ в этом процессе выступает операционная система Astra Linux Special Edition. Однако академическая среда, в частности программы магистратуры, зачастую продолжает базироваться на изучении проприетарных зарубежных решений. Это формирует заметный разрыв между навыками, которые получают выпускники, и реальным стеком технологий, используемым работодателями в государственном секторе и на объектах критической информационной инфраструктуры. В связи с этим возникает острая необходимость адаптации учебных курсов по защите информации к архитектурным реалиям отечественных операционных систем.

Основная часть

Компетентностный разрыв в подготовке специалистов обусловлен фундаментальными архитектурными различиями платформ. Многолетнее использование Windows сформировало у студентов паттерны, опирающиеся исключительно на дискреционное управление доступом и графические инструменты администрирования.

Сравнительный анализ подходов к администрированию, определяющих специфику образовательных программ, представлен в таблице.

Сравнительный анализ подходов к администрированию безопасности
Comparative analysis of security administration approaches

Характеристика	Традиционный подход (на примере семейства Windows)	Импортозамещающий подход (на примере Astra Linux)
Базовая модель разграничения доступа	Дискреционная (списки ACL файловой системы NTFS)	Мандатная (подсистема PARSEC, встроенная в ядро)
Изоляция процессов и данных	Базовая изоляция на уровне сессий пользователей	Изоляция по мандатным уровням и категориям конфиденциальности
Управление программной средой	Преимущественно через групповые политики (GPO) и стороннее антивирусное ПО	Нативная замкнутая программная среда (ЗПС) с проверкой цифровых подписей (ELF-файлов)

Переход на новую парадигму требует глубокого понимания логики работы с мандатными метками, контекстом безопасности процессов и принципами доверенного сеанса. Специалист, обученный на зарубежных ОС, на практике не готов к настройке мандатного контроля целостности или администрированию встроенных средств защиты Astra Linux без стороннего ПО.

Для преодоления барьера требуется системный пересмотр лабораторного практикума. Ключевым принципом адаптации выступает полное погружение обучающихся в нативную среду ОС через интерфейс командной строки. Студенты должны изучить утилиты для работы с мандатными атрибутами (pdpl-file, pdp-ls), научиться настраивать графические киоски и организовывать замкнутую программную среду (ЗПС), блокирующую запуск файлов без соответствующих цифровых подписей.

Апробация обновленных модулей в магистерских дисциплинах показала высокую эффективность. Смещение фокуса оценочных средств на практическую локализацию инцидентов (например, выявление нарушения целостности файлов) улучшило результаты аттестации. Отчеты по практике подтверждают, что студенты четко осознают взаимосвязь архитектуры ОС и требований по защите информации.

Заключение

Переход ИТ-инфраструктуры на отечественные решения выявляет существенный компетентностный дефицит среди молодых специалистов, вызванный архитектурной спецификой мандатного управления доступом. Эффективная подготовка кадров для работы с Astra Linux невозможна без концептуальной перестройки образовательных программ. Системное внедрение в учебный процесс лабораторных практикумов, ориентированных на глубокое взаимодействие со встроенными механизмами защиты (включая подсистему PARSEC), позволяет значительно повысить уровень практической подготовки выпускников и ускорить их профессиональную адаптацию.

Список использованных источников

1. Буренин П. Н., Девянин П. Н., Колесников А. В. (2021) Безопасность операционной системы специального назначения Astra Linux Special Edition. Москва, Издательство «Горячая линия – Телеком».
2. Щербаков А. Ю. (2022) Современные операционные системы: архитектура и механизмы защиты. Москва, Издательство «Горячая линия – Телеком».
3. Смирнов С. Н. (2024) Импортзамещение в сфере информационных технологий: вызовы для системы высшего образования. Вестник педагогических наук. (2), 15–22.

References

1. Burenin P. N., Devyanin P. N., Kolesnikov A. V. (2021) Security of the Special Purpose Operating System Astra Linux Special Edition. Moscow, Goryachaya liniya – Telekom Publishing House (in Russian).
2. Shcherbakov A. Yu. (2022) Modern Operating Systems: Architecture and Security Mechanisms. Moscow, Goryachaya liniya – Telekom Publishing House (in Russian).
3. Smirnov S. N. (2024) Import Substitution in the Field of Information Technology: Challenges for the Higher Education System. Bulletin of Pedagogical Sciences. (2), 15–22 (in Russian).

Сведения об авторе

Бердник А.И., инженер электросвязи, ООО «Альпиндустрия», berdnik1326547@gmail.com.

Information about the author

Berdnik A.I., Telecommunications Engineer, Alpindustria LLC, berdnik1326547@gmail.com.

УДК 004.056.53

АРХИТЕКТУРА ТЕХНИЧЕСКОЙ ЗАЩИТЫ И ВЫБОР ДОВЕРЕННОЙ ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ ИЗМЕРИТЕЛЬНЫХ IoT-СИСТЕМ

П.К. Маевский

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается актуальная проблема технической защиты измерительных устройств Интернета вещей (IoT) на аппаратном уровне. Обосновывается необходимость внедрения концепции доверенной среды на этапе проектирования, что особенно критично при выводе новых продуктов на рынок. Предложен подход к выбору микроконтроллеров с аппаратной поддержкой криптографических стандартов Республики Беларусь (СТБ 34.101.31) для обеспечения целостности и конфиденциальности передаваемых данных.

Ключевые слова: техническая защита информации; измерительные системы; доверенная среда; аппаратное шифрование; микроконтроллеры; интернет вещей; криптографические алгоритмы; СТБ 34.101.31; сертификация; кибербезопасность.

ARCHITECTURE OF TECHNICAL PROTECTION AND SELECTION OF TRUSTED ELEMENT BASE FOR MEASURING IoT-SYSTEMS

P.K. Mayeuski

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article deals with the urgent problem of technical protection of Internet of Things (IoT) measuring devices at the hardware level. The necessity of implementing the trusted environment concept at the design stage is justified, which is especially critical

when launching new products. An approach to selecting microcontrollers with hardware support for cryptographic standards of the Republic of Belarus (STB 34.101.31) to ensure the integrity and confidentiality of transmitted data is proposed.

Keywords: technical information protection; measuring systems; trusted environment; hardware encryption; microcontrollers; internet of things; cryptographic algorithms; STB 34.101.31; certification; cybersecurity.

Введение

Стремительный рост количества подключенных устройств Интернета вещей (IoT), включая промышленные и бытовые измерительные приборы, формирует новые вызовы в области технической защиты информации. Датчики телеметрии, умные счетчики и различные трекеры все чаще становятся объектами кибератак, направленных на подмену данных или перехват управления. Разработка аппаратных измерительных устройств, в том числе в рамках подготовки бизнес-плана для вывода на рынок новых технологических стартапов, требует закладки архитектуры безопасности еще на этапе базового проектирования. Отсутствие такого подхода делает невозможным прохождение экспертизы в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь и внедрение приборов на критически важных объектах. Целью данной работы является формирование концепции выбора доверенной элементной базы для измерительных систем.

Основная часть

Современные портативные измерительные приборы обладают ограниченными вычислительными ресурсами и жесткими рамками энергопотребления. При этом передаваемые телеметрические данные должны защищаться с использованием сертифицированных криптографических алгоритмов, в частности, в соответствии с СТБ 34.101.31. Программная реализация ресурсоемких алгоритмов на слабых микроконтроллерах (MCU) приводит к быстрому разряду батареи устройства и недопустимым задержкам в передаче данных.

Эффективным решением данной проблемы является концепция «доверенной среды» (Trusted Execution Environment) на аппаратном уровне. В архитектуру измерительного прибора необходимо закладывать SoC (System-on-a-Chip) или микроконтроллеры, имеющие встроенные аппаратные криптографические сопроцессоры, физически изолированную память для хранения ключей и защиту портов отладки (JTAG). В общем виде процесс формирования криптограммы для защиты конфиденциальности данных измерительного прибора в режиме сцепления блоков можно выразить формулой:

$$C_i = E_K(P_i \oplus C_{i-1}), \quad (1)$$

где C_i – текущий блок шифротекста; E_k – функция аппаратного шифрования на ключе K (например, по стандарту BelT); P_i – блок открытых телеметрических данных; $\oplus$ – операция побитового сложения по модулю 2; C_{i-1} – предыдущий блок шифротекста.

Аппаратная реализация функции E_k позволяет существенно снизить нагрузку на центральный процессор прибора по сравнению с программной реализацией [1]. Кроме того, физическое разделение зон памяти предотвращает несанкционированное считывание прошивки или модификацию калибровочных коэффициентов измерительного датчика даже при наличии физического доступа к устройству. Выбор компонентной базы должен осуществляться с учетом необходимости минимизации рисков наличия недеklarированных возможностей в зарубежных микросхемах [2].

Заключение

Интеграция аппаратных модулей безопасности в архитектуру измерительных приборов является обязательным условием для создания конкурентоспособного и защищенного продукта. Для инженерных команд, разрабатывающих новые приборы учета или контроля параметров среды, применение микроконтроллеров с аппаратной поддержкой отечественных криптографических стандартов значительно упрощает процедуру сертификации и допуска к эксплуатации на объектах информационной инфраструктуры Республики Беларусь.

Список использованных источников

1. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. (2003) Математические и компьютерные основы криптологии. Минск, Издательство «Новое знание».
2. Малюк А. А. (2020) Теория защиты информации. Москва, Издательство «Горячая линия-Телеком».

References

1. Kharin Yu. S., Bernik V. I., Matveev G. V., Agievich S. V. (2003) Mathematical and Computer Foundations of Cryptology. Minsk, Novoe Znanie Publishing House (in Russian).
2. Malyuk A. A. (2020) Information Security Theory. Moscow, Goryachaya Liniya-Telecom Publishing House (in Russian).

Сведения об авторе

Маевский П. К., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mmauglik1113@gmail.com.

Information about the author

Maevsky P. K., Cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, mmauglik1113@gmail.com.

УДК 004.41

ПРИМЕНЕНИЕ АНСАМБЛЕВЫХ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ФИЛЬТРАЦИИ ЛОЖНЫХ СРАБАТЫВАНИЙ В SIEM-СИСТЕМАХ

А.Г. Бокун

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассмотрена проблема высокой доли ложных срабатываний в современных системах мониторинга событий информационной безопасности (SIEM). Во введении обоснована актуальность внедрения легковесных механизмов автоматизации для снижения нагрузки на операторов систем защиты. В основной части приведено описание типовой архитектуры ядра SIEM-системы и выделены ключевые этапы обработки данных, на которых возможно внедрение инструментов машинного обучения. Предложено решение на основе алгоритма «Случайный лес», сочетающее в себе устойчивость к переобучению и прозрачность принятия решений за счет оценки важности параметров. В заключении сделан вывод о преимуществе использования ансамблей решающих деревьев перед тяжеловесными нейросетевыми моделями при решении задач классификации инцидентов в локальных сетях.

Ключевые слова: информационная безопасность, SIEM-система, ложные срабатывания, машинное обучение, классификация событий, случайный лес, корреляция событий.

APPLICATION OF ENSEMBLE MACHINE LEARNING METHODS FOR FALSE POSITIVE FILTERING IN SIEM

A.G. Bokun

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article addresses the issue of high false positive rates in modern Security Information and Event Management (SIEM) systems. The introduction substantiates the relevance of implementing lightweight automation mechanisms to reduce the workload on security operations center (SOC) analysts. The main body describes the typical architecture of a SIEM core and identifies key data processing stages where machine learning tools can be effectively integrated. The author proposes a solution based on the Random Forest algorithm, which combines resistance to overfitting with decision-making transparency through feature importance evaluation. The conclusion emphasizes the advantages of using decision tree ensembles over heavyweight neural network models for incident classification tasks within local networks.

Keywords: information security, SIEM, false positives, machine learning, event classification, random forest, event correlation.

Введение

Вопрос защиты информации является сегодня одним из приоритетных направлений для всех хозяйствующих субъектов. Разные экономические агенты обладают разным количеством данных, которые необходимо защищать, и разными возможностями эту защиту имплементировать. Если малому бизнесу достаточно просто соблюдать базовые правила информационной безопасности, то большим предприятиям с разветвленной внутренней информационной сетью не обойтись без комплексных решений вроде SIEM систем.

Архитектура таких систем хорошо известна и прошла проверку временем, однако она имеет ряд недостатков, которые можно решить с помощью современных подходов. Одним из таких недостатков являются ложные срабатывания. Цель работы предложить легковесный механизм для решения проблемы обнаружения ложных событий информационной безопасности в SIEM системах на основе алгоритмов машинного обучения.

Основная часть

В начале считаем необходимым кратко рассмотреть общую архитектуру современных SIEM систем (их ядра) для определения наиболее оптимального места, где можно имплементировать решение.

Для сбора данных такие системы используют два основных подхода: агентный и безагентный сбор. По сути эти методы отличаются необходимостью установки дополнительного ПО на целевой узел: агентные системы предполагают установку приложения-агента на узел, который активно собирает данные и отправляет их в аналитические центры системы. Безагентные системы полагаются на пассивный сбор данных через протоколы вроде syslog и чтение обобщенных файлов (если речь идет про Windows).

После непосредственного сбора данных об узле информация пересылается в аналитическое ядро SIEM-системы (далее просто ядро), где проходят несколько этапов обработки. Обобщая эти этапы, их можно обозначить следующим образом.

1. Нормализация – процесс приведения разрозненных данных к общей форме, которая описана правилами нормализации. Правила определяют какие поля должны быть в конечной структуре и как с ними далее работать.

2. Агрегация – процесс объединения похожих событий в одно. Здесь система сверяется с правилами агрегации и приводит группировку однородных данных в единые сущности.

3. Корреляция – процесс выявления инцидентов безопасности на основе некоторого контекста событий. Система наработала окно агрегированных событий и может проверить его на наличие событий, образующих инцидент безопасности (согласно правилам корреляции). После чего оператор оповещается о созданном событии.

Помимо трех основных этапов иногда встречаются дополнительные, в их число могут входить следующие.

1. Обогащение – процесс добавление дополнительных метаданных скоррелированному инциденту, как правило используются заранее прописанные в правилах обогащения источники дополнительной информации.

2. Добавление контекста – система помогает рассматривать инциденты не как отдельные происшествия, а ставить их в общий аналитический контекст.

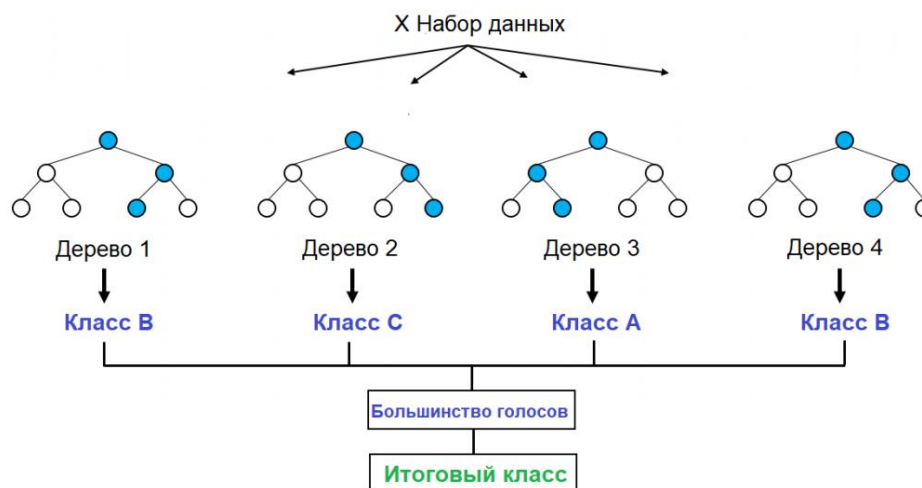
Современные SIEM-системы обладают широким перечнем интеллектуальных инструментов, однако основной расчет все еще делается на корректное написание правил. Обнаружение инцидентов информационной задачи – крайне комплексная и персонифицированная задача, условия которой меняются от одной сети к другой. Невозможно дать одно универсальное решение, поэтому специалисты по информационной безопасности работают отдельно с каждой сетью, учитывают их специфику и с помощью правил затачивают SIEM под конкретную задачу. Такая гибкость является несомненным преимуществом, однако тут же появляется и проблема – правила нельзя написать идеально, поэтому время от времени происходят ложные срабатывания – система реагирует на легальную активность, которая тем не менее попала под ее правила корреляции.

Данная проблема стоит крайне остро в рутине оператора SIEM-систем, так как специалист вынужден тратить свое время на поиск и закрытие ложных срабатываний вместо того чтобы заниматься мониторингом. Полноценной автоматизации решения этой проблемы на рынке все еще нет: некоторые системы (Wazuh) оставляют все на откуп оператору, некоторые (MaxPatrol, KUMA) предлагают довольно тяжеловесные решения на основе полноценных нейронных сетей, которые впрочем больше подходят под решение более глобальных и общих задач. В связи с этим предлагаем свое решение на основе легких моделей машинного обучения.

Определим тип решаемой задачи. Имеется некоторая фиксированная структура данных, данная структура заполняется однородной информацией. Необходимо разделить объекты этой структуры на два класса, для текущей задачи это «ложное срабатывание» и «не ложное срабатывание». То есть это задача классификации с неизменной

структурой данных. Для решения данного типа задач обычно используются модели на основе деревьев принятий решений и градиентный бустинг.

Однако стоит отметить, что важным требованием к модели является прозрачность принятия решений. То есть оператор должен точно понимать, почему модель выбрала тот или иной вариант, чтобы принять конечное информированное решение. Такой набор требований делает модели на основе решающих деревьев более применимыми. Конкретно мы предлагаем модель, которая называется «случайный лес». Случайный лес – это модель машинного обучения, которая использует ансамбль случайных деревьев для создания предсказаний. Решением всего ансамбля будет среднее решение деревьев, входящих в него. Упрощенная схема работы случайного леса представлен на рисунке.



Общая схема работы модели случайного леса
The general scheme of the random forest model

В модели случайного леса есть две политики принятия решений: жесткое и мягкое голосование:

- жесткое голосование – каждый классификатор (решающее дерево) делает предсказание, а предсказанием ансамбля (случайного леса) будет решение, за которое проголосовало большинство;

- мягкое голосование – каждый классификатор предоставляет процентку с вероятностями принятия того или иного решения, в этом случае суммирующий механизм ансамбля при принятии окончательного решения учитывает не сами голоса моделей, а именно полученные вероятности.

Архитектурно случайный лес крайне устойчив к переобучению, что важно, так как обучающая выборка будет довольно однородной (так как обучение будет происходить на данных конкретной сети). Также важным аспектом является то, что оно может продемонстрировать

коэффициент важности параметров, это делает решения более прозрачными и помогает оператору при аналитике инцидентов.

Заключение

В итоге можно сказать, что предложенный подход решает проблему перегрузки операторов SIEM-систем ложными срабатываниями за счет внедрения легковесного механизма классификации на базе машинного обучения. Выбор модели «Случайный лес» обоснован ее устойчивостью к переобучению и способностью ранжировать важность параметров, что обеспечивает необходимую прозрачность принятия решений. В отличие от тяжеловесных нейросетей, такой алгоритм легче адаптируется к специфике конкретной сети и позволяет специалистам сосредоточиться на анализе реальных инцидентов.

Список использованных источников

1. Ахикян А.И., Данилюк С.С. (2024) Алгоритм машинного обучения адаптивный случайный лес и его применение. *Вестник науки*. (75), 1393-1402.
2. Цымбал Ф.А. (2022) Управление инцидентами безопасности и событиями (SIEM). *Столыпинский вестник*. (4), 2121-2129.

References

1. Akhikyan, A. I., & Danilyuk, S. S. (2024). Adaptive Random Forest Machine Learning Algorithm and Its Application. *Vesnik Nauki*, (75), 1393-1402.
2. Tsymbal, F. A. (2022). Security Information and Event Management (SIEM). *Stolypinskiy Vestnik*, (4), 2121-2129.

Сведения об авторе

Бокун А.Г., магистрант, ассистент кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.bokun@bsuir.by.

Information about the author

Bokun A., Master Student, Assistant at the Informatics Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.bokun@bsuir.by.

УДК 004.75:004.056

СИСТЕМА ПОДТВЕРЖДЕНИЯ ТРАНЗАКЦИЙ В БЛОКАХ ПУБЛИЧНЫХ БЛОКЧЕЙН-СЕТЕЙ

А.А. Буневич

*Учреждение образования «Белорусская государственная академия связи»,
г. Минск, Республика Беларусь*

Аннотация. Статья посвящена проблеме неэффективности традиционного механизма ускорения транзакций в блоках публичных блокчейн-сетей. В работе предлагается концепция архитектуры для оптимизации подтверждения транзакций, основанной на комбинации метода Replace-By-Fee, машинного обучения и распределенной файловой системы. Рассмотренный алгоритм, анализирует исторические и реальные данные о состоянии блокчейна, прогнозирует оптимальные комиссии для ускорения включения транзакций в блоки, а также автоматически корректирует их в процессе подтверждения. Данный подход позволяет существенно сократить время подтверждения транзакций, снизить процент отклоненных и количество неуспешных операций по сравнению с традиционными подходами.

Ключевые слова: блокчейн; Replace-By-Fee; оптимизация подтверждения транзакций; адаптивные алгоритмы; машинное обучение; распределенная файловая система; сетевая нагрузка; динамическое управление транзакциями.

TRANSACTION CONFIRMATION SYSTEM IN BLOCKS OF PUBLIC BLOCKCHAIN NETWORKS

A.A. Bunevich

*Educational Institution "Belarusian State Academy of Communications",
Minsk, Republic of Belarus*

Abstract. The article addresses the issue of inefficiency in the traditional mechanism for accelerating transactions within blocks of public blockchain networks. The paper proposes an architectural concept for optimizing transaction confirmation, based on a combination of the Replace-By-Fee method, machine learning, and a distributed file system. The discussed algorithm analyzes historical and real-time blockchain state data, predicts optimal fees to accelerate the inclusion of transactions in blocks, and automatically adjusts them during the confirmation process. This approach significantly reduces transaction confirmation time and lowers the rate of rejected and failed operations compared to traditional methods.

Keywords: blockchain; Replace-By-Fee; transaction confirmation optimization; adaptive algorithms; machine learning; distributed file system; network load; dynamic transaction management.

Введение

Стремительное развитие технологий распределенного реестра и их интеграция в различные сферы экономической деятельности обусловили повышение требований к производительности и надежности публичных блокчейн-сетей. Стандартные механизмы, такие как статические комиссии за транзакции и ограниченное место в блоке для транзакций, часто неэффективны в условиях изменчивой сетевой нагрузки и динамически

сменяющегося спроса на операции. Это приводит к длительному ожиданию подтверждения, повышенным комиссиям и риску невыполнения транзакций, особенно при пиковых нагрузках.

Основная часть

Традиционный подход к ускорению подтверждения – механизм Replace-By-Fee (далее – RBF) – позволяет отправителю увеличить комиссию уже отправленной неподтвержденной транзакции, чтобы ускорить ее включение в блок [1]. Однако этот механизм, как правило, реализуется вручную или с использованием статических правил, что не обеспечивает оптимального баланса между скоростью, стоимостью и надежностью операции. Необходимость в автоматизации и адаптации комиссий к текущим рыночным и сетевым условиям становится очевидной [2].

Ключевым элементом предложенной архитектуры является модель адаптивного RBF на основе машинного обучения. Данная модель обучается на исторических данных: истории транзакций, включая время отправки, первоначальную комиссию, динамику изменения комиссии, время ожидания подтверждения и фактическое включение в блок. С помощью регрессионных и классификационных алгоритмов модель учитывает множество факторов: текущую загрузку сети, исторические тенденции, сезонность, динамику цены комиссии в зависимости от времени суток или дня недели [3–4]. На основе этого анализа для каждой новой транзакции модель формирует оптимальное значение комиссии, максимизирующее вероятность ее быстрого включения в следующий блок [5].

Для эффективной работы адаптивных алгоритмов используется модуль прогнозирования состояния блокчейна и сети. Информация собирается из публичных нод и аналитических сервисов блокчейна, а также из логов собственной системы. На их основе формируются рекомендации по динамической настройке параметров транзакций [6].

Для обеспечения централизации, но при этом высокой доступности и безопасности метаданных используется распределенное хранение на базе таких технологий, как IPFS (InterPlanetary File System) или распределенные базы данных. Каждая транзакция и ее текущий статус, история изменений комиссии, попытки подтверждения и метаданные о сети хранятся в распределенной файловой системе. Такая архитектура позволяет не только быстро получать доступ к историческим данным для обучения моделей, но и обеспечивает резервирование и синхронизацию данных между узлами сети блокчейна [7].

Процесс работы предлагаемой системы начинается с анализа входящей транзакции: модуль определяет текущее состояние сети

блокчейна, исторические тенденции и параметры транзакции. Затем машинное обучение модель вычисляет оптимальную начальную комиссию и стратегию возможного изменения комиссии через RBF в зависимости от прогнозируемого состояния блока и сети. После отправки транзакции система мониторит ее статус в реальном времени с помощью распределенного хранилища. Если транзакция не подтверждается в ожидаемые сроки, модель динамически рекомендует или автоматически инициирует новую RBF-операцию с повышенной комиссией. Все события фиксируются в распределенной базе данных, что позволяет не только отслеживать историю, но и постоянно улучшать модели адаптации.

Реализация предложенной архитектуры, также требует тесной интеграции с узлами блокчейна, поддержки API для получения актуальных данных о блоках и транзакциях, а также механизмов безопасности для защиты метаданных от несанкционированного доступа и манипуляций. Организованная асинхронная обработка событий обеспечивает минимальную задержку при принятии решений о корректировке комиссии.

Также необходимо обратить внимание масштабируемости решения. Архитектура, основанная на микросервисах и распределенных компонентах, позволяет легко добавлять новые узлы для обработки и хранения данных, а также масштабировать модели машинного обучения при росте объема транзакций. Интеграция с популярными платформами блокчейна через стандартные API, облегчает внедрение решения в уже существующие экосистемы [8].

Важно отметить, что предлагаемая система не затрагивает консенсус-механизмы самих блокчейнов, а фокусируется на оптимизации поведения участников и инструментов для повышения эффективности транзакционного процесса на уровне пользовательских и операторских операций.

Заключение

Использование адаптивных алгоритмов позволяет минимизировать время ожидания подтверждения, снижать стоимость транзакций и повышать их успешную надежность даже при экстремальных нагрузках. Модульная структура архитектуры обеспечивает гибкость, масштабируемость и безопасность хранения метаданных. В перспективе такая оптимизация может стать частью стандартного набора инструментов для блокчейновых платформ, способствуя повышению их привлекательности для широкого круга пользователей и разработчиков.

Список использованных источников

1. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. – Новосибирск: ИМ СО РАН, 2016. – 350 с.

2. Мищенко В.А., Мищенко А.В. Распределенные системы хранения данных: учебное пособие. – СПб.: Университет ИТМО, 2019. – 124 с.
3. Назаров Д.М., Петров А.А. Блокчейн-технологии в цифровой экономике. – М.: ИНФРА-М, 2020. – 208 с.
4. Орехов И.А., Васильев Д.В. Машинное обучение в задачах обработки данных финансовых рынков. – М.: ЛЕНАНД, 2018. – 240 с.
5. Соколов И.А. Технологии распределенного реестра: блокчейн. – М.: ИНФРА-М, 2021. – 192 с.
6. Талалаев А.В., Иванов П.В. Методы оптимизации транзакций в блок-чейн-системах. – СПб.: НИУ ИТМО, 2020. – 168 с.
7. Филимонов А.Е. Интеллектуальные системы управления блокчейн-сетями. – М.: МЦНМО, 2019. – 256 с.
9. Шумский С.А. Распределенные вычисления и блокчейн. – М.: Горячая линия-Телеком, 2020. – 320 с.

References

1. Zagoruiko N.G. Applied Methods of Data and Knowledge Analysis. – Novosibirsk: Institute of Mathematics SB RAS, 2016. – 350 p.
2. Mishchenko V.A., Mishchenko A.V. Distributed Data Storage Systems: A Tutorial. – St. Petersburg: ITMO University, 2019. – 124 p.
3. Nazarov D.M., Petrov A.A. Blockchain Technologies in the Digital Economy. – Moscow: INFRA-M, 2020. – 208 p.
4. Orekhov I.A., Vasiliev D.V. Machine Learning in Financial Market Data Processing Tasks. – Moscow: LENAND, 2018. – 240 p.
5. Sokolov I.A. Distributed Ledger Technologies: Blockchain. – Moscow: INFRA-M, 2021. – 192 p.
6. Talalaev A.V., Ivanov P.V. Methods for Optimizing Transactions in Blockchain Systems. – St. Petersburg: NRU ITMO, 2020. – 168 p.
7. Filimonov A.E. Intelligent Control Systems for Blockchain Networks. – Moscow: MCCME, 2019. – 256 p.
8. Shumsky S.A. Distributed Computing and Blockchain. – Moscow: Hotline-Telecom, 2020. – 320 p.

Сведения об авторах

Буневиц А.А., аспирант, учреждения образования «Белорусская государственная академия связи», kndraleks@gmail.com.

Information about the authors

Bunevich A.A., Postgraduate Student, Educational Institution "Belarusian State Academy of Communications", kndraleks@gmail.com.

UDC 004.05

DEVELOPMENT OF MATHEMATICAL TOOLS FOR IMAGE RESTORATION WITH DISTORTED DATA

Jing Wang

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This paper addresses image restoration in the presence of Gaussian noise, salt and pepper noise, occlusion and blur. A review of mathematical methods-from Fourier filters and statistical hypothesis testing to regression trees-is presented. The research aims to develop a unified framework for image quality assessment integrating statistical rigor with computational techniques.

Keywords: image; restoration; statistical hypothesis testing; Kolmogorov-Smirnov test; Gaussian noise; salt and pepper noise; blur; regression tree methods; occlusion; quality assessment.

Introduction

Images serve critical roles from medical diagnostics to forensic investigation, but their integrity is frequently compromised during acquisition, transmission, and storage. Restoration of images with missing or corrupted data represents a fundamental challenge. Unlike noise corruption, which perturbs pixel values while preserving structure, missing data scenarios involve complete absence of information in affected regions – common in medical imaging artifacts, satellite transmission errors, and historical photograph damage.

The novelty of this research lies in its comparison of mathematical methodologies for image quality assessment. While existing literature explores individual restoration techniques, a gap remains in comprehensive comparative analysis evaluating statistical hypothesis testing methods across diverse distortion types and sample sizes.

Main Part

Image recovery reconstructs missing or corrupted regions algorithmically. The degradation model is expressed as:

$$g(x, y) = M(x, y) \cdot f(x, y) + n(x, y), \quad (1)$$

where $f(x, y)$ – the original image; $g(x, y)$ – the observed image; $M(x, y)$ – a binary mask indicating known ($M = 1$) and missing ($M = 0$) regions; $n(x, y)$ – additive noise.

Four distortion types are considered. Gaussian noise follows a normal distribution affecting all pixels, resulting from sensor noise. Salt and pepper noise manifests as random extreme pixel values (0 or 255) due to transmission errors. Occlusion represents complete loss of original information in affected

regions. Blur reduces sharpness through convolution with a point spread function from camera motion or defocus.

Statistical methods use hypothesis testing to determine whether a distorted image maintains statistical similarity to the original. The Kolmogorov-Smirnov (KS) test is a non-parametric test comparing two probability distributions:

$$D = \sup_x |F_1(x) - F_2(x)|, \quad (2)$$

where F_1 and F_2 – empirical cumulative distribution functions.

If D exceeds a critical value, the null hypothesis that samples come from the same distribution is rejected.

The Anderson-Darling test gives more weight to distribution tails, detecting differences in extremes. The Shapiro-Wilk test for normality is effective for small to moderate sample sizes, verifying assumptions before applying parametric methods.

Other Approaches. Regression tree methods learn patterns from training data, capturing non-linear relationships between image features (mean, variance, skewness, kurtosis) and quality metrics. Fourier filter methods operate in the frequency domain, with the Wiener filter minimizing mean square error. Variational methods formulate recovery as optimization balancing data fidelity with regularization constraints.

Existing Software Analysis. Adobe Photoshop provides professional restoration but requires manual tuning and lacks statistical assessment. MATLAB offers comprehensive functions but needs programming expertise. OpenCV provides efficient implementations without automated quality assessment. Deep learning frameworks enable state-of-the-art restoration but require extensive training data and computational resources.

Research Objectives. This research develops a framework for image restoration with distorted data, addressing identified limitations. Tasks include: analysis of existing mathematical methods; development of a unified framework integrating multiple approaches; and systematic experimental validation across distortion types and sample sizes. Preliminary analysis indicates statistical hypothesis testing methods tolerate higher defect rates for Gaussian noise and blur than regression tree methods, providing interpretable results valuable for scientific applications.

Conclusion

This paper has presented an overview of image recovery, covering Gaussian noise, salt and pepper noise, occlusion, and blur. Review of Fourier filters, statistical hypothesis testing (KS, Anderson-Darling, Shapiro-Wilk tests), and regression trees revealed strengths and limitations. Analysis of existing

software tools identified common shortcomings motivating unified framework development.

References

1. Gonzalez R. C., Woods R. E. (2018) *Digital Image Processing*. 4th ed. New York, Pearson.
2. Massey F. J. (1991) The Kolmogorov-Smirnov Test for Goodness of Fit. *Journal of the American Statistical Association*. 46 (253), 68–78.
3. Shapiro S. S., Wilk M. B. (1995) An Analysis of Variance Test for Normality. *Biometrika*. 52 (3/4), 591–611.
4. Breiman L., Friedman J. H., Olshen R. A., Stone C. J. (1984) *Classification and Regression Trees*. Belmont, Wadsworth.

Information about the authors

Wang J., master's student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, qiaonu38@gmail.com.

УДК 621.317.7:004.056.5

АНАЛИЗ ПАРАМЕТРОВ ПРИБОРОВ ОБНАРУЖЕНИЯ СКРЫТЫХ ПРОВОДОВ ТЕХНИЧЕСКИХ СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ С ПОМОЩЬЮ КОМПЛЕКСНОГО ГЕОМЕТРИЧЕСКОГО ПОКАЗАТЕЛЯ КАЧЕСТВА

В.М. Алефиренко, Е.Д. Зубрицкий, А.Н. Морозова

Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Выполнена оценка технических характеристик тепловизионных приборов с использованием комплексного геометрического показателя качества. Проведен сравнительный анализ моделей, выделены устройства с наилучшими параметрами.

Ключевые слова: защита информации; несанкционированный съем информации; скрытые провода; детекторы проводов; комплексный геометрический показатель качества; сравнительный анализ; технические характеристики; оценка качества; приборы обнаружения; анализ параметров.

ANALYSIS OF HIDDEN WIRE DETECTOR PARAMETERS USING A COMPLEX GEOMETRIC QUALITY INDICATOR

V.M. Alefirenko, E.D. Zubritsky, A.N. Morozova

*Educational Institution «Belarusian State University of Informatics and
Radioelectronics», Minsk, Republic of Belarus*

Abstract. The evaluation of technical characteristics of thermal imaging devices has been performed using a complex geometric quality indicator. A comparative analysis of models has been carried out, and the devices with the best parameters are identified.

Keywords: information security; unauthorized information interception; hidden wires; wire detectors; complex geometric quality indicator; comparative analysis; technical characteristics; quality assessment; detection devices; parameter analysis.

Введение

Для поиска технических средств несанкционированного съема информации, управляемых по проводам (микрофоны, стетоскопы, видеокамеры), в системы защиты информации необходимо включать детекторы скрытых проводов.

Основная часть

В работе [1] представлен сравнительный анализ характеристик приборов обнаружения скрытых проводов с помощью комплексного арифметического показателя качества. Наряду с ним существует геометрический показатель, определяемый по формуле

$$K_{\text{геом}} = \sqrt[m]{\prod_{i=1}^m k_{\text{Hi}}^{\alpha_{\text{Hi}}}}, \quad (1)$$

где k_{Hi} – нормированный i -й единичный показатель; α_{Hi} – нормированный коэффициент значимости i -го единичного показателя; m – количество единичных показателей, принятых во внимание.

Для приведения параметров к безразмерному виду применяется нормировка

$$K_{\text{Hi}} = \frac{k_i - k_{\text{кр } i}}{k_{\text{опт } i} - k_{\text{кр } i}}, \quad (2)$$

где k_i – исходное значение i -го показателя; $k_{\text{кр } i}$ – критическое значение i -го единичного показателя; $k_{\text{опт } i}$ – оптимальное значение i -го показателя; $k_{\text{max } i}$ – максимальное значение i -го показателя; $k_{\text{min } i}$ – минимальное значение i -го показателя.

Исходные значения k_i должны лежать в пределах $k_{\text{кр } i} < k_i < k_{\text{опт } i}$ или $k_{\text{опт } i} < k_i < k_{\text{кр } i}$. Коэффициенты значимости α_{Hi} для формулы (1) должны выбираться таким образом, чтобы обеспечивалось соблюдение условия

$$\prod_{i=1}^m \alpha_{\text{Hi}} = 1, \quad (3)$$

тогда нормированные значения α_{Hi} будут лежать в пределах $0 < \alpha_{\text{Hi}} < 1$.

Представляет интерес исследование с помощью геометрического показателя [2] и сравнение результатов [3]. Как и в работе [1], для сравнения выбраны восемь моделей детекторов проводов различных фирм: *Bosch GMS 120 Professional*, *Bosch GMS 100 M Professional*, *ADA Instruments Wall Scanner 80*, *ADA Instruments Wall Scanner 50*, ЗУБР

Мастер DX-350, ЗУБР Профессионал DX-750, *Laserliner CombiFinder Plus 080.955A*, *Wortex MD 3009*.

Учитывались характеристики: максимальная глубина обнаружения, количество программ, время работы, габариты, вес, рабочие температуры, гарантийный срок, цена и др. Результаты расчетов по формулам (1)–(3) представлены на рисунке.



Распределение комплексных геометрических показателей качества приборов обнаружения скрытых проводов
Distribution of Complex Geometric Quality Indicators of Hidden Wire Detectors

Первые три места заняли: *ADA Instruments Wall Scanner 80* (0,61), *Bosch GMS 120 Professional* (0,56) и *Bosch GMS 100 M Professional* (0,46). Эти же модели лидируют и по арифметическому показателю.

Заключение

Сравнение восьми детекторов по геометрическому показателю подтвердило сходимость с арифметическим методом и позволяет рекомендовать данный подход для выбора оптимальных средств поиска.

Список использованных источников

1. Алефиренко, В.М. Сравнительный анализ технических характеристик приборов обнаружения скрытых проводов технических средств несанкционированного съема информации / В.М. Алефиренко, А.Д. Денскевич, Е.Д. Зубрицкий // Технические средства защиты информации : материалы XXIII Междунар. науч.-техн. конф., Минск, 8 апр. 2025 г. – Минск : БГУИР, 2025. – С. 55–58.
2. Алефиренко, В.М. Анализ технических характеристик металлодетекторов с помощью комплексного геометрического показателя качества / В.М. Алефиренко, А.Д. Денскевич, Е.Д. Зубрицкий // Сетевое издание «Научные исследования XXI века». – 2025. – № 1 (33), – С. 6–10.
3. Алефиренко, В.М. Выбор состава технических средств для систем обеспечения безопасности / В.М. Алефиренко // Доклады БГУИР. – 2017. – № 2 (104). – С. 39–44.

References

1. Alefirenko, V.M. Comparative analysis of technical characteristics of hidden wire detectors for unauthorized information interception equipment / V.M. Alefirenko, A.D. Denskevich, E.D. Zubritsky // Technical Means of Information Protection : Proceedings of the XXIII International Scientific and Technical Conference, Minsk, April 8, 2025. – Minsk : BSUIR, 2025. – P. 55–58..
2. Alefirenko V.M., Denskevich A.D., Zubritsky E.D. Analysis of technical characteristics of metal detectors using a complex geometric quality indicator. Online publication "Scientific Research of the XXI Century", 2025, No. 1 (33), pp. 6–10.
3. Alefirenko V.M. Selection of technical means composition for security systems. Doklady BSUIR, 2017, No. 2 (104), pp. 39–44.

Сведения об авторах

Алефиренко В.М., канд. техн. наук, доц., доц. каф. ПИКС, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alefirenko@bsuir.by.

Зубрицкий Е.Д., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», zzubritski@gmail.com.

Морозова А.Н., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», annamorozova417@gmail.com.

Information about the authors

Alefirenko V.M., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Infocommunication Systems, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, alefirenko@bsuir.by.

Zubritsky E.D., Master's Student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, zzubritski@gmail.com.

Morozova A.N., Master's Student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, annamorozova417@gmail.com.

УДК 004.001

АЛГОРИТМ ПОСТКВАНТОВОГО ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ И ПРИНЦИПА КУБИКА РУБИКА

А.В. Сидоренко, И.В. Сергеев

*Белорусский государственный университет,
г. Минск, Республика Беларусь*

Аннотация. В работе приведены основные аспекты гибридного алгоритма постквантового шифрования изображений, основанного на 3D-хаотической системе и принципе Кубика Рубика. Для создания криптографически стойкого алгоритма предложено объединить преимущества хаотических систем и квантовых вычислений.

Представлены основные особенности разработанного алгоритма в виде компьютерной программы.

Ключевые слова: постквантовое шифрование, изображение, хаотические системы, принцип Кубика Рубика.

POSTQUANTUM IMAGE ENCRYPTION ALGORITHM WITH CHAOTIC SYSTEM AND RUBIK'S CUBE PRINCIPLE

A.V. Sidorenko, I.V. Sergeev

Belarusian State University, Minsk, Republic of Belarus

Abstract. The main aspects of combine the advantages new 3D-chaotic system and quantum computing based on a modified Lorenz system for generating pseudorandom keys and Rubik's Kyber principle for perform image scrambling operations (cyclic shifting of row and column) is used. The main features, structure and properties of created algorithm are received as computer program.

Keywords: post-quantum encoding; image; chaotic system; Rybic's Kyber principle

Введение

С появлением новых квантовых вычислительных систем возникает необходимость перехода к новым методам криптографии, способным обеспечить надежную защиту в квантовую эпоху [1,2]. При шифровании изображений, характерным для которых является обработка большого объема данных, возникает необходимость перехода к новым методам защиты информации, так как существующие традиционные методы типа RSA, ECC не обладают соответствующими свойствами. При использовании постквантового шифрования, представляющего собой семейство криптографических алгоритмов, устойчивых к атакам как со стороны классических, так и квантовых компьютеров, возникает проблема совместимости.

Одним из перспективных инновационных направлений является использование хаотических систем для генерации псевдослучайных ключей и реализации процедур перемешивания и диффузии данных. В данной работе предлагается объединить преимущества квантовой криптографии и хаотических алгоритмов, используя квантовую модель представления изображения и принцип Кубика Рубика для реализации эффективного алгоритма шифрования.

Алгоритм на основе хаотической системы и принципа Кубика Рубика

Современные методы защиты информации все чаще применяют идеи из смежных областей, включая динамические системы и комбинаторную математику.

Кубик Рубика представляет собой пластмассовый куб (форм-фактор в первоначальном варианте $3 \times 3 \times 3$). Его видимые элементы снаружи выглядят как 54 грани малых кубиков, составляющих один большой куб, и способны вращаться вокруг трех внутренних осей куба. Поворачивая строки и столбцы кубика можно осуществлять циклически сдвиг строк и столбцов. Основываясь на этом, эффект шифрования изображения может быть достигнут путем циклического перемешивания строк и столбцов в процессе шифрования [3]. Полученные путем сдвига блоки могут быть представлены в виде массивов пикселей элементов шифруемого изображения. С математической точки зрения поворот граней кубика аналогичен применению матрицы перестановки к множеству векторов, описывающих значения составляющих интенсивностей цвета (RGB- (R- red (красный), G-green (зеленый), B- blue (голубой)). За счет рекурсивных итеративных перестановок в криптографии принцип Кубика Рубика позволяет достичь высокой степени спутанности и рассеяния информации. Спутанность при этом достигается за счет частых перестановок пикселей между блоками, а рассеяние – за счет воздействия на значения цветовых компонентов (в частности, за счет побитовой операции-XOR с псевдослучайными последовательностями).

Важную роль играют хаотические отображения, применяемые в процессе управления поворотами, например, отображение Кота Арнольда, логистическое отображение [4]. Многократное применение выбранного отображения обеспечивает равномерную перестановку пикселей.

Программная реализация алгоритма

В данной работе реализация алгоритма проводится в виде компьютерной программы следующим образом:

Разработана программная реализация алгоритма квантового шифрования изображений, основанная на предложенной новой хаотической системе и принципе Кубика Рубика, обеспечивающих устойчивость к атакам и высокую степень запутанности данных.

Оптимизирован алгоритм обработки изображений с использованием многопоточности, что позволило сократить время выполнения шифрования и повысить производительность системы.

Созданы квантовые схемы с применением библиотеки Quiskit для представления изображения, осуществления операции трансляции и диффузии, а также моделирования квантовых вычислений на симуляторе Aersimulator.

Проведено тестирование корректности работы алгоритма, визуального анализа результатов и сравнения зашифрованных изображений с целью подтверждения соответствия реализации требованиям безопасности

и эффективности. Важную роль играют хаотические отображения, применяемое в процессе управления поворотами, например, отображение кота Арнольда, логистическое отображение.

Для реализации алгоритма шифрования на языке программирования Python использовались следующие библиотеки:

```
Import numpy as np
import cv2
from qiskit import Quantum Circuit, Quantum Register, Classical Register,
transpile
from qiskit import AerSimulator
from math import ceil, log2
import concurrent.futures
import os
```

где `numpy(np)` –используется для работы с массивами, создания ключей и хранения значений изображения, `cv2 (Open CV)` –библиотека для работы с изображениями, используется для чтения изображения и преобразования его в нужные форматы, `Quiskit` -библиотека для создания квантовых схем. В коде используются: `Quantum Circuit`, `Quantum Register`, `Classical Register` – создание и работа с классическими и квантовыми регистрами. `Transpile`-преобразование схемы в оптимизированную форму для симуляции или выполнения на реальном квантовом компьютере. `AerSimulator` –симулятор квантовых схем от `Quiskit`, `math` –используются функции для математических вычислений – (`ceil`, `log2`), `concurrent.futures` –позволяет обрабатывать блоки изображения параллельно с помощью многопоточности, `Qs` –используется для получения числа процессоров при многопоточности.

Следует отметить, что библиотека `Quiskit` разработана компанией IBM и в нашем исследовании была использована как платформа для моделирования и анализа алгоритма квантового шифрования изображений. Для определения работоспособности и надежности работы алгоритма проведено тестирование разработанной программы. Тестирование проводилось на черно-белых и цветных тестовых изображениях, имеющих различные размеры.

Проведенный анализ показал, что в результате работы исследуемого алгоритма коэффициент корреляции соседних пикселей, рассчитанных в горизонтальном, вертикальном и диагональном направлениях оригинальных и зашифрованных изображений близок к нулю, что усложняет прослеживание закономерностей пикселей.

Выполненный энтропийный анализ, проведенный с использованием симуляционных данных показал, что рассматриваемый алгоритм является

устойчивым к атакам, так как информационная энтропия близка к идеальной величине, равной восьми.

Заключение

В работе рассматривается гибридный алгоритм квантового шифрования изображений, основанный на хаотической системе и принципе Кубика Рубика и его программная реализация. Программная реализация выполнена на языке Python, а также с использованием библиотек: Quiskit, Open CV и Numpy. Визуальный и гистограммный анализ показал равномерное распределение пикселей в зашифрованных изображениях, а также отсутствие корреляции между соседними пикселями.

Список использованных источников

1. Kiktenko E.O (2018) Quantum Sequired Blockchain. *ArXiv:1795.09258.v.3[quant]*3 Jan20181.
2. Belklur M (2022) Quantum vs Classic Computing. A Comparative Analysis *Sevens International Conference on Fog and Mobile Edge Computing*, Pars, France, IEEE, p. 1-8.
3. Landhaoukha R.A. Secure Image Algorithm Based on Rubik's Cube Principle. *Journal of Electric Computer Engineering* Article ID 173931(13)
4. Сидоренко А.В. (2016) Информационные системы на основе динамического хаоса. Минск, Издательство БГУ.

References

1. Kiktenko E.O (2018) Quantum Sequired Blockchain. *ArXiv:1795.09258.v.3[quant]*3 Jan20181.
2. Belklur M (2022) Quantum vs Classic Computing. A Comparative Analysis *Sevens International Conference on Fog and Mobile Edge Computing*, Pars, France, IEEE, p. 1-8.
3. Landhaoukha R.A. Secure Image Algorithm Based on Rubik's Cube Principle. *Journal of Electric Computer Engineering* Article ID 173931(13)
4. Sidorenko A.V. (2016) *The Information Systems Based on Dynamic Chaos. Minsk, Belarusian State University* (in Russian)

Сведения об авторах

Сидоренко А. В., д-р техн. наук, проф. проф, Белорусский государственный университет, SidorenkoA@yandex.by.

Сергеев И. В., студент 4 курса факультета радиофизики и компьютерных технологий, Белорусский государственный университет.

Information about the authors

Sidorenko A.V., Dr. Sci. (Tech.), professor, professor, Belarusian State University, sidorenkoA@yandex.by

Sergeev I.V., student, faculty of radiophysics and electronics, Belarusian State University.

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБНАРУЖЕНИЯ BRUTE-FORCE АТАК В СИСТЕМАХ АУТЕНТИФИКАЦИИ

Т.А. Мельникова, В.В. Васькевич

*Учреждение образования «Гомельский Государственный университет
имени Франциска Скорины», г. Гомель, Республика Беларусь*

Аннотация. В статье рассматриваются основные подходы к обнаружению атак методом полного перебора в системах аутентификации. Проводится сравнительный анализ пороговых, статистических методов, методов на основе машинного обучения, поведенческого анализа и гибридных подходов. Для каждого метода определены преимущества и недостатки. Сформулированы рекомендации по выбору метода в зависимости от архитектуры системы и модели угроз.

Ключевые слова: технические средства защиты информации; brute-force атака; обнаружение атак; угроза; уязвимости; система аутентификации; механизмы защиты; информационная безопасность; машинное обучение; системы обнаружения вторжений.

COMPARATIVE ANALYSIS OF EXISTING METHODS FOR DETECTING BRUTE-FORCE ATTACKS IN AUTHENTICATION SYSTEMS

T.A. Melnikova, V.V. Vaskevich

*Educational Institution "Francysk Skaryna Gomel State University", Gomel,
Republic of Belarus*

Abstract. The article discusses the main approaches to detecting brute-force attacks in authentication systems. A comparative analysis of threshold methods, statistical methods, machine learning-based methods, behavioral analysis and hybrid approaches is carried out. Advantages and disadvantages are defined for each method. Recommendations on the choice of the method are formulated depending on the architecture of the system and the threat model.

Keywords: technical means of information protection; brute-force attack; attack detection; threat; vulnerabilities; authentication system; protection mechanisms; information security; machine learning; intrusion detection systems.

Введение

Атаки методом полного перебора остаются одной из наиболее распространенных угроз для систем аутентификации. Несмотря

на кажущуюся примитивность, они продолжают эволюционировать. Классические механизмы защиты все чаще оказываются недостаточными – они либо создают вектор для denial-of-service атак на легитимных пользователей, либо пропускают распределенные атаки, в которых количество попыток с одного IP-адреса удерживается ниже порога.

Основная часть

Для предотвращения brute-force атак применяются пороговые, статические, методы на основе машинного обучения, поведенческий анализ, методы на основе CAPTCHA и proof-of-work, методы на основе анализа графов и репутации.

Пороговые методы основаны на подсчете неудачных попыток аутентификации за заданное время и сравнении с установленным порогом. При его достижении происходит блокировка учетной записи либо ограничение числа запросов с одного IP-адреса. Метод прост в реализации, требует минимальных вычислительных ресурсов и эффективен против нераспределенных атак. Однако он уязвим к распределенным атакам и password spraying, при которых ни один IP-адрес или учетная запись не набирает достаточного числа неудачных попыток. Выбор порога неоднозначен: низкое значение ведет к блокировке легитимных пользователей, высокое – к пропуску атак.

Статистические методы анализируют отклонения паттернов аутентификации от модели нормального поведения, учитывая не только количество неудачных попыток, но и характеристики распределения запросов. К основным подходам относятся: анализ на основе распределения запросов (например, пуассоновского), метод кумулятивных сумм для обнаружения изменений в потоке событий, анализ энтропии целевых учетных записей и IP-адресов, а также последовательный анализ Вальда с контролируемым уровнем ошибок. Эти методы обладают более высокой точностью, способны обнаруживать медленные атаки и password spraying. Вместе с тем они требуют периода обучения, чувствительны к изменениям легитимного поведения и сложнее в настройке [1].

Методы на основе машинного обучения автоматически строят модели классификации или обнаружения аномалий, выявляя сложные нелинейные зависимости в данных. Обучение с учителем использует размеченные наборы данных с примерами атак, обучение без учителя обнаруживает аномалии как отклонения от нормального кластера. Учитываемые признаки включают число и соотношение неудачных попыток, интервалы между ними, число уникальных целевых записей с одного IP, географию источников, характеристики User-Agent и другие. Методы ML обеспечивают высокую точность обнаружения распределенных

и адаптивных атак, однако зависят от качества обучающих данных, требуют значительных вычислительных ресурсов, подвержены переобучению и снижению точности при изменении стратегий атакующих.

Поведенческий анализ строит профиль нормального поведения каждого пользователя и обнаруживает отклонения от него, учитывая временные и географические паттерны, характеристики устройств, ритм набора пароля и сетевые параметры. Метод эффективен при обнаружении credential stuffing и password spraying, устойчив к адаптации атакующего и минимизирует ложноположительные срабатывания. К недостаткам относятся высокие требования к хранению данных, проблемы конфиденциальности и снижение точности при изменении привычек пользователя [2].

CAPTCHA требует решения задачи, трудной для автоматизации, reCAPTCHA v3 присваивает оценку риска без явного взаимодействия с пользователем, proof-of-work требует выполнения вычислительно затратной операции. Эти методы увеличивают стоимость атаки, но не обнаруживают ее – они лишь замедляют перебор. При этом классические CAPTCHA ухудшают процесс погружения пользователя в процесс, а существующие сервисы и ML-алгоритмы позволяют обходить многие их виды.

Методы на основе анализа графов и репутации моделируют взаимосвязи между IP-адресами, учетными записями и устройствами в виде графа, выявляя аномальные структуры. IP-репутация использует внешние базы для оценки риска источника, а коллективная разведка угроз (Threat Intelligence) обеспечивает обмен индикаторами компрометации. Методы эффективны при обнаружении координированных распределенных атак и ботнетов, однако зависят от актуальности репутационных баз и дают ложные срабатывания при использовании VPN легитимными пользователями.

Гибридные методы объединяют несколько подходов для компенсации индивидуальных недостатков – например, пороговый метод отсеивает очевидные атаки, а ML-модель анализирует оставшийся трафик. Такой подход обеспечивает наивысшую точность и устойчивость к обходу, позволяет адаптировать архитектуру под конкретную модель угроз и поэтапно внедрять новые компоненты. Основные ограничения – сложность внедрения и сопровождения, увеличение задержки обработки запросов и высокая стоимость разработки и эксплуатации.

Заключение

Проведенный сравнительный анализ показывает, что ни один метод не является универсальным. Пороговые методы достаточны для простых

атак, но неэффективны против распределенных и адаптивных угроз. Методы машинного обучения демонстрируют наивысшую точность, однако ограничены проблемами качества данных и вычислительными затратами. Поведенческий анализ наиболее устойчив к адаптации атакующего, но требует значительных инвестиций. Оптимальным решением для большинства систем является гибридный подход, комбинирующий методы различных категорий, однако при этом стоимость защиты должна быть соизмерима стоимости защищаемых активов и ожидаемому ущербу от успешной атаки.

Список использованных источников

1. Марков А. С., Цирлов В. Л. (2020) Выявление аномалий в сетевом трафике с использованием статистических методов и кумулятивных сумм. Безопасность информационных технологий. 27(2), 34–45.
2. Ольков С. А. (2021) Поведенческий анализ пользователей в системах непрерывной аутентификации. Проблемы информационной безопасности. Компьютерные системы. (1), 60–68.

References

1. Markov A. S., Tsirlov V. L. (2020) Detection of anomalies in network traffic using statistical methods and cumulative sums. Information Technology Security. 27(2), 34–45 (in Russian).
2. Olek S. A. (2021) Behavioral analysis of users in continuous authentication systems. Problems of information security. Computer systems. (1), 60–68 (in Russian).

Сведения об авторах

Мельникова Т.А., студентка 4 курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования «Гомельский Государственный университет имени Франциска Скорины», mva_tanya@mail.ru.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский Государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Melnikova T., 4nd year student of the Faculty of Physics and Information Technology specialty “Computer security”, Francysk Skaryna Gomel State University, mva_tanya@mail.ru.

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Francysk Skaryna Gomel State University, vaskevich@gsu.by.

УДК 004.312

RS-ЗАЩЕЛКА КАК ИСТОЧНИК СЛУЧАЙНОСТИ В РЕЖИМЕ ИНИЦИАЛИЗАЦИИ

М.Н. Кайки, А.А. Иванюк

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В работе выполнен анализ значений инициализации RS-защелки, реализованной на базе ПЛИС, в котором показано, что разброс задержек в межсоединениях, обусловленный различиями в маршрутах трассировки, является определяющим фактором в получении случайных последовательностей.

Ключевые слова: RS-защелка; метастабильность; задержка распространения; источник энтропии; физически неклонлируемая функция (ФНФ); автоколебания, ПЛИС;

RS-LATCH AS A SOURCE OF RANDOMNESS IN INITIALIZATION MODE

M.N. Kaiky, A.A. Ivaniuk

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The work analyzes the initialization values of an RS latch implemented on an FPGA, which shows that the spread of delays in interconnections, caused by differences in routing paths, is a determining factor in obtaining high randomness characteristics.

Keywords: RS latch; metastability; propagation delay; entropy source; physically unclonable function (PUF); oscillations; FPGA;

Введение

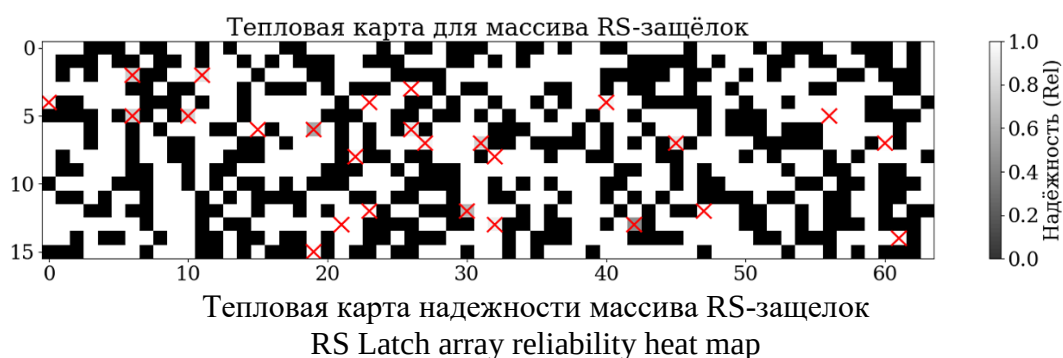
Реализация генераторов истинно случайных чисел (ГИСЧ) на базе программируемых логических интегральных схем (ПЛИС) требует использования полностью цифровых источников энтропии, способных функционировать в условиях жестких аппаратных ограничений [1]. Среди перспективных источников выделяются бистабильные элементы памяти, поведение которых при нарушении временных соотношений становится недетерминированным [2]. Архитектура ПЛИС характеризуется наличием разветвленной сети коммутационных ресурсов, вносящих технологически зависимые задержки распространения сигналов [3]. Автоматизированная трассировка приводит к различию задержек в плечах обратной связи RS-защелки, нарушая симметрию элемента. Цель работы – анализ влияния вариативности задержек в цепях межсоединений ПЛИС на переход RS-защелки в метастабильное состояние для использования в качестве источника энтропии в аппаратных ГИСЧ в режиме инициализации при включении питания.

Эксперимент по инициализации RS-защелки

Проведем эксперимент, в котором покажем зависимость параметра надежности ФНФ на базе RS-защелки. Для проведения эксперимента будем перезагружать экземпляр ПЛИС (Xilinx Zynq-7020 в составе платы быстрого прототипирования PYNQ Z2) K раз, где $K = 500$ и после каждой перезагрузки считывать значения с выхода Q_i из 1024 ячеек RS-защелок, где i – индекс защелки. Тогда надежность для каждой ячейки рассчитывается так:

$$Rel_i = 2 \left| \frac{\sum_{k=0}^{K-1} Q_{ik}}{K} - 0,5 \right|, \quad (1)$$

где K – количество циклов перезагрузки ПЛИС; Q_{ik} – ответ i -той RS-защелки в цикле перезагрузки k .



Как видно из рисунка, у большинства ячеек (97,5%) между циклами перезагрузки ответы соответствовали $Rel=1$ и формировали подобие уникального и стабильного отпечатка экземпляра ПЛИС, однако у оставшихся 2,5% RS-защелок надежность $Rel < 1$.

При помощи инструментов netlist-моделирования системы автоматизированного проектирования Vivado был получен файл, предназначенный для хранения и передачи информации о задержках и временных характеристиках электронных схем – SDF (Standard Delay Format). Анализ временных параметров показал, что задержки на цепях межсоединений значительно превышают задержки на логических элементах (LUT6). В среднем, задержки маршрутизации больше в 9 раз, что свидетельствует о доминирующем вкладе межсоединений в общую асимметрию временных характеристик аппаратной реализации RS-защелки.

Заключение

Полученные результаты позволяют сформулировать ряд выводов, имеющих значение для развития физических методов генерации случайных чисел в полностью цифровых средах. Проведенное исследование подтвердило, что основным источником недетерминированного поведения RS-защелок при включении питания является не только внутренний шум полупроводниковой структуры, а и технологически обусловленная асимметрия задержек в цепях межсоединений. Автоматизированная трассировка, выполняемая системами проектирования, неизбежно вносит различия в длины маршрутов обратной связи. Практическая значимость полученных результатов заключается в возможности создания гибридных архитектур, совмещающих на одном кристалле функции идентификации и генерации случайных чисел. Исследование демонстрирует, что сложность и неоднородность современных ПЛИС, традиционно рассматриваемые как недостаток, могут быть обращены в преимущество при создании физических источников энтропии. Технологический разброс, неизбежный при производстве и автоматизированном проектировании, становится не препятствием, а основой для реализации криптографических примитивов, опирающихся на неконтролируемые физические процессы.

Список использованных источников

1. Gassend B., Clarke D., Van Dijk M., Devadas S. Silicon Physical Random Functions. *Proc. of the 9th ACM conference on Computer and communications security, CCS '02*. 2002:148-160
2. Technical specification Physical random number generators for use in cryptographic information protection tools that do not contain information constituting a state secret: TS 26.4.001-2019: valid from 18.04.2019 / Technical Committee for Standardization "Cryptographic Information Protection". - Moscow 2019. - 20 p.
3. Ivanyuk, A. A. Physically non-cloneable Arbiter-type function with non-linear path pairs / A. A. Ivanyuk, A. Yu. Shamina // *Systems Analysis and Applied Informatics*. - 2023. - No. 1. - P. 54-62.

References

1. Gassend B., Clarke D., Van Dijk M., Devadas S. Silicon Physical Random Functions. *Proc. of the 9th ACM conference on Computer and communications security, CCS '02*. 2002:148-160
2. Technical specification Physical random number generators for use in cryptographic information protection tools that do not contain information constituting a state secret: TS 26.4.001-2019: valid from 18.04.2019 / Technical Committee for Standardization "Cryptographic Information Protection". - Moscow 2019. - 20 p.

3. Ivanyuk, A. A. Physically non-cloneable Arbiter-type function with non-linear path pairs / A. A. Ivanyuk, A. Yu. Shamina // Systems Analysis and Applied Informatics. - 2023. - No. 1. - P. 54-62.

Сведения об авторах

Кайки М.Н., магистр техн. наук, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kaikymykhailo@gmail.com

Иваниук А.А., д-р техн. наук, проф., проф. каф. информатики, «Белорусский государственный университет информатики и радиоэлектроники», ivaniuk@bsuir.by

Information about the authors

Kaiky M. N., M. Sci. (Tech.), Educational Institution "Belarusian State University of Informatics and Radioelectronics", kaikymykhailo@gmail.com

Ivaniuk A. A., Dr. Sci. (Tech.), Professor, Professor at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ivaniuk@bsuir.by

UDC 004.052.42

EXTRACTING DATA FROM THE HASH MEMORY USING AN ERROR KEY

M.H. Nguyen, Yu.O. German

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This paper addresses the problem of retrieving data from hash memory using erroneous keys. Propose a character-level Convolutional Neural Network (CNN) model that corrects misspelled input words before hash table lookup. Approach generates synthetic errors (deletion, insertion, transposition) with up to two modifications from a base vocabulary of 10 words. The model encodes input strings as character sequences, applies embedding and 1D convolution layers, and classifies them into the correct word classes. Experimental results show high accuracy in correcting common typing errors, demonstrating the feasibility of using neural networks as a preprocessing layer for fault-tolerant hash memory systems.

Keywords: character-level; CNN; accuracy; hash memory; fault-tolerant; deletion; insertion; transposition; tensorflow; epoch.

Introduction

Hash memory enables fast data retrieval but requires exact key matching, making it vulnerable when keys contain spelling errors. This paper proposes a character-level Convolutional Neural Network (CNN) that corrects erroneous keys before hash table access, using synthetic errors (deletion, insertion, transposition) for training. Experimental results on a 10-word vocabulary demonstrate that our approach achieves high accuracy in correcting keys with up to two errors, offering a fault-tolerant solution for hash-based memory systems.

Main Part

In hash-based memory systems, even a single character error in the lookup key leads to either a cache miss or retrieval of incorrect data. Traditional error correction methods (e.g., Hamming codes) work at the bit level but cannot handle semantic errors in human-generated keys.

Existing approaches include Edit distance (Levenshtein, 1966), Phonetic algorithms (Soundex, Metaphone), Neural approaches (Kim et al., 2016), and BERT-based correction (Devlin et al., 2019). Unlike these methods that require dictionary lookup or large language models, our CNN-based classifier offers a balance between speed and accuracy for fixed-vocabulary hash key correction.

Simulate three common error types:

- deletion: remove a character (e.g., apple → aple);
- insertion: add a random character (e.g., apple → appple);
- transposition: swap adjacent characters (e.g., apple → papple).

CNN architecture consists of:

- embedding layer: 32-dimensional character embeddings;
- conv1D: 64 filters, kernel size 3, ReLU activation;
- global Max Pooling: Extract most salient features;
- dense layers: 64 neurons (ReLU) followed by 10-class softmax.

Experiments were conducted on a CPU with 16GB RAM. The model was implemented using TensorFlow 2.x. Character-level CNN model has evaluated on 200 randomly generated test samples (20 per word). The figure 1 shows the training progress over 5 epochs.

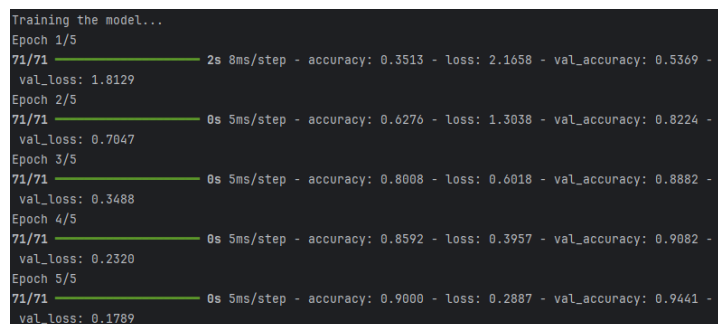


Figure capture: Training and validation accuracy over 5 epochs

The model achieved: accuracy by word: apple – 90.00% (18/20); banana – 100.00% (20/20); orange – 100.00% (20/20); grape – 95.00% (19/20); peach – 100.00% (20/20); cherry – 100.00% (20/20); lemon – 90.00% (18/20); mango – 100.00% (20/20); berry – 100.00% (20/20); melon – 75.00% (15/20).

Summary of findings: overall test accuracy: 95.0%; validation accuracy: 94.4%; training accuracy: 90.0%; words with 100% accuracy: 8/10; lowest accuracy: 75% (melon).

Conclusion

This paper has proposed a character-level CNN for correcting erroneous keys in hash memory systems, achieving 95.0% accuracy on synthetic errors with up to two modifications. The model successfully handles deletion, insertion, and transposition errors while maintaining sub-millisecond inference time, making it suitable for real-time preprocessing.

References

1. Devlin J., Chang M. W., Lee K., Toutanova K. (2019) BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of NAACL-HLT*, 4171–4186.
2. Kim Y., Jernite Y., Sontag D., Rush A. M. (2016) Character-aware neural language models. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, 2741–2749.

Information about the authors

Nguyen M.H., Master’s student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, minhhiiep452001@gmail.com.

German Yu.O., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Technologies of Automated Systems, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, jgerman@bsuir.by.

УДК 004.056.5

АППАРАТНЫЕ ФУНКЦИИ БЕЗОПАСНОСТИ В ФОРМИРОВАНИИ РЫНОЧНОЙ СТОИМОСТИ IT-ПЛАТФОРМ

А.К. Крамаренко, Н.Д. Егоренков

Учреждение образования «Брестский государственный технический университет», г. Брест, Республика Беларусь

Аннотация. Актуальность работы – повышение числа атак в контексте физического доступа к устройствам и необходимость изучения значимости аппаратных функций безопасности для степени защищенности и рыночной стоимости IT-платформ. В статье приводятся результаты исследования некоторых аппаратных механизмов безопасности в экосистеме Apple (iOS, iPadOS, macOS). Приведено их сравнение с Android и Windows. Внимание уделено механизмам доверенной нагрузки, аппаратного шифрования, защиты памяти устройств. Выделены преимущества глубокой интеграции Apple над TPM 2.0, Titan M/C и TrustZone.

Ключевые слова: аппаратная безопасность; Secure Enclave; Apple Silicon; физические атаки; trusted execution environment; биометрическая аутентификация; шифрование данных.

HARDWARE SECURITY FUNCTIONS IN DETERMINING THE MARKET VALUE OF IT PLATFORMS

A.K. Kramarenko, M.D. Yahorenkau

*Educational Institution “Brest State Technical University”, Brest, Republic of
Belarus*

Abstract. The relevance of this article lies in the increasing number of attacks involving physical access to devices, and the consequent necessity to examine the significance of hardware security features regarding both the level of protection and the market value of IT platforms. This article presents the results of a study examining specific hardware security mechanisms within the Apple ecosystem (iOS, iPadOS, and macOS), comparing them with those found in Android and Windows. Particular attention is devoted to mechanisms for trusted boot, hardware encryption, and device memory protection. The advantages of Apple's deep integration approach relative to TPM 2.0, Titan M/C, and TrustZone are highlighted.

Keywords: hardware security; Secure Enclave; Apple Silicon; physical attacks; trusted execution environment; biometric authentication; data encryption.

Введение

В современных условиях защита от несанкционированного доступа приобретает все большее значение. Угрозы зачастую связаны с физическим доступом к устройству: evil maid, cold boot, прямое извлечение содержимого памяти. Традиционные программные механизмы становятся уязвимыми. В связи с этим, переход к аппаратным функциям безопасности, встроенным в процессор, является необходимым для развития IT-платформ [1]. Экосистема Apple на базе чипов Apple Silicon и модуле Secure Enclave Processor является наиболее эффективной благодаря глубокой аппаратно-программной интеграции. Актуальность работы определяется повышением числа атак в контексте физического доступа к устройствам и необходимостью изучения значимости аппаратных функций безопасности для степени защищенности и рыночной стоимости IT-платформ. Цель – исследовать некоторые аппаратные механизмы безопасности в современных IT-платформах (на примере экосистемы Apple).

Основная часть

В условиях цифровизации информационная безопасность – это важный фактор, влияющий на доверие пользователей, и, следовательно, на рыночную стоимость IT-платформ [1]. В качестве примера рассмотрим экосистему Apple.

Экосистема Apple (iOS, iPadOS, macOS) работает на принципе аппаратно-программной интеграции. Центральный элемент – Secure Enclave Processor (SEP). Он работает независимо от основного CPU. Также

в нем хранятся криптографические ключи, биометрические шаблоны Face ID / Touch ID и выполняются операции шифрования. Такие ключи остаются в SEP, даже при полном компрометировании операционной системы. Apple Secure Boot позволяет проверить цифровую подпись – от Boot ROM до ядра ОС. Аппаратное шифрование данных (AES-256) включается автоматически [2]. В чипах Apple Silicon (М-серия) и T2 (в старых Intel-маках) также есть Pointer Authentication (PAC), который защищает указатели от атак. Биометрические ключи Face ID / Touch ID создаются и хранятся в SEP, их извлечение практически невозможно даже при физическом доступе к устройству.

Далее сравним в данном контексте Android и Windows [2]. В Android основной механизм – ARM TrustZone. Он генерирует доверенную среду выполнения (TEE). В устройствах Google Pixel также используется отдельный чип Titan M2. Он хранит ключи, изучает целостность загрузки. При этом из-за фрагментации платформы (разные производители) уровень интеграции ниже, чем у Apple. Для сравнения, в Windows – TPM 2.0 (дискретный или firmware-вариант). Он контролирует загрузку и хранение ключей для BitLocker. В некоторых устройствах также есть и Microsoft Pluton (аналог Secure Enclave). Исследование позволило выделить некоторые преимущества Apple. Ключевым является такое, как: SEP связан с SoC и ОС (обеспечивается максимальная защита от physical access-атак (evil maid, cold boot, прямое чтение памяти)). В Android и Windows модульный подход влияет на гибкость системы, в тоже время он увеличивает уязвимость при физическом доступе (ключи извлекаются из наименее изолированных компонентов) [3]. Проведенное исследование показало, что аппаратный уровень Apple формирует наибольшую устойчивость у к атакам физического доступа. Его конкуренты, предлагают открытые, но менее защищенные решения.

Заключение

Проведенный анализ позволяет сделать следующие выводы. Технически глубокая интеграция обеспечивает Apple большую защиту от физических атак. Модульные архитектуры Android и Windows схожи по функциям, но уступают Apple в устойчивости из-за фрагментации и меньшей изоляции некоторых компонентов. В бизнес-аспекте позиционирование устройств Apple создает премиальный сегмент бренда. Android и Windows ищут баланс между открытостью системы и защитой. Также, на наш взгляд, изолированная архитектура Apple упрощает выполнение требований регуляторов. А ключи шифрования Apple физически недоступны для ОС. В Android и Windows в этом контексте требуются дополнительные настройки и сторонние средства. Таким образом, при повышении интенсивности атак с физическим доступом

аппаратная безопасность – это фундамент доверия. В Apple синергия инженерных решений задает планку, к которой вынуждены подстраиваться конкуренты.

Список использованных источников

1. Крамаренко А. К., Русенко В. Н. (2024) Интеграция программного обеспечения в бизнес: процесс, проблемы и перспективы. Интеллектуальные ресурсы – региональному развитию. (1), 232–237.
2. Костяйнен К., Дхар А., Чапкун С. (2020) Выделенные чипы безопасности в эпоху защищенных анклавов. IEEE Security & Privacy. 18 (5), 38–46. (На англ. яз.).
3. Равичандран Дж. (2023) Обнаружение новых микроархитектурных уязвимостей безопасности в современных процессорах. Магистерская диссертация, Массачусетский технологический институт. (На англ. яз.).

References

1. Kramarenko A. K., Rusenko V. N. (2024) Integration of Software into Business: Process, Problems and Prospects. Intellectual Resources – Regional Development. (1), 232–237 (in Russian).
2. Kostianen K., Dhar A., Chapkun S. (2020) Trusted Hardware in the Era of Secure Enclaves. IEEE Security & Privacy. 18 (5), 38–46 (in English).
3. Ravichandran J. (2023) Discovering New Microarchitectural Security Vulnerabilities in Modern Processors. Master’s Thesis, Massachusetts Institute of Technology (in English).

Сведения об авторах

Крамаренко А.К., канд. экон. наук, доц., доц. кафедры бухгалтерского учета, анализа и аудита, учреждение образования «Брестский государственный технический университет», annnakramarenko@yandex.by

Егоренков Н.Д., студент факультета электронно-информационных систем, учреждение образования «Брестский государственный технический университет», egorenkovnikita0@gmail.com.

Information about the authors

Kramarenko A.K., Cand. Sci. (Econ.), Associate Professor, Associate Professor of the Department of Accounting, Analysis, and Audit, Educational Institution “Brest State Technical University”, annnakramarenko@yandex.by

Yahorenkau N.D., student, Faculty of Electronic Information Systems, Educational Institution “Brest State Technical University”, egorenkovnikita0@gmail.com.

УДК 004.056.5

МЕТОДЫ ЗАЩИТЫ АЛГОРИТМА BelT ОТ АТАК С ВНЕДРЕНИЕМ ОШИБОК

А.С. Герасимов, К.Е. Макаренко

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В работе исследуется уязвимость алгоритма блочного шифрования BelT к атакам с внедрением ошибок. Рассмотрен математический принцип дифференциальной атаки на последний раунд шифрования BelT-128, позволяющий восстановить секретный ключ по четырем успешным внедрениям ошибок. Выполнена оценка вычислительной сложности. Проанализированы методы защиты аппаратных реализаций.

Ключевые слова: BelT, атаки по сторонним каналам, внедрение ошибок, fault injection, дифференциальный анализ.

A METHODS OF PROTECTING THE BELT ALGORITHM FROM ATTACKS WITH FAULTS

A.S. Gerasimov, K.E. Makaranka

*Educational Institution «Belarusian State University of Informatics and
Radio Electronics», Minsk, Belarus*

Abstract. The paper investigates the vulnerability of the BelT block encryption algorithm to error injection attacks. It considers the mathematical principle of a differential attack on the last round of BelT-128 encryption, which allows for the recovery of the secret key based on four successful error injections. The computational complexity is evaluated. The methods for protecting hardware implementations are analyzed.

Keywords: BelT, side-channel attacks, error injection, fault injection, and differential analysis.

Введение

Алгоритм блочного шифрования BelT утвержден в качестве государственного стандарта Республики Беларусь СТБ 34.101.31-2020 [1]. BelT используется в смарт-картах, токенах, модулях безопасности. При атаке с внедрением ошибок злоумышленник воздействует на устройство, вызывая сбой в вычислениях, и по разности правильного и ошибочного результатов восстанавливает ключ. В 2015 году исследователи из Университета Пассау, Германия, опубликовали работу, в которой показали, что BelT уязвим к таким атакам [2]. Для BelT-128 требуется 4 успешных внедрений ошибок. Это означает, что при физическом доступе к устройству злоумышленник может легко восстановить ключ. В данной работе продемонстрируем математический принцип атаки с внедрением ошибок на BelT-128 и предложим решение данной проблемы.

Основная часть

Атака основана на дифференциальном анализе ошибок. Рассмотрим последний (8-й) раунд шифрования BelT-128. В этом раунде используются два ключевых слова θ_7 и θ_8 (32 бита каждое). В BelT-128 выполняется соотношение $\theta_7 = \theta_3$, $\theta_8 = \theta_4$ [1].

В позицию L_1 (рисунок 1) внедряется ошибка f_1 , которая может изменить произвольное количество битов в 32-разрядном слове. Наблюдая правильный шифротекст Y и ошибочный шифротекст Y' , можно получить значения f_1 и разность на выходе.

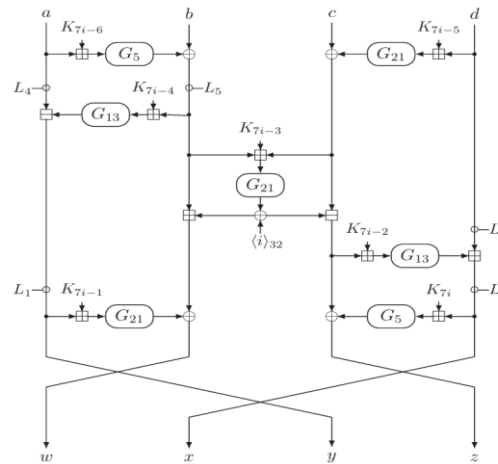


Схема алгоритма BelT
The scheme of the BelT algorithm

Пусть:

$Y = (w, x, y, z)$ – правильный шифротекст (4 слова по 32 бита);

$Y' = (w', x', y', z')$ – ошибочный шифротекст

L_1 – значение в точке внедрения ошибки;

$f_1 = y \oplus y'$ – значение ошибки (наблюдаемая разность);

$\Delta w = w \oplus w'$ – разность на выходе в позиции w .

Получаем уравнение:

$$G_{21}(L1 \oplus \theta_7) \oplus G_{21}((L1 \oplus f1) \oplus \theta_7) = \Delta w \quad (1)$$

Все величины в уравнении (1), кроме θ_7 , известны. $L_1 = y$, $f_1 = y \oplus y'$, $\Delta w = w \oplus w'$ из правильного и ошибочного шифротекстов.

Уравнение (1) позволяет отфильтровать возможные значения θ_7 . Для каждого из 2^{32} возможных значений θ (от 0 до $2^{32}-1$) вычислим левую часть уравнения и сравним с правой частью Δw . Из θ , при которых выполняется равенство, будет составлено множество отобранных кандидатов как Θ_7 . Аналогично для θ_8 .

При внедрении ошибки в позицию L_2 (соответствующую x) и анализе разности $\Delta z = z \oplus z'$ получаем уравнение для θ_8 :

$$G_{13}(L_2 \oplus \theta_8) \oplus G_{13}((L_2 \oplus f_2) \oplus \theta_8) = \Delta z \quad (2)$$

где $f_2 = x \oplus x'$, $L_2 = x$.

Аналогичные процедуры выполняются для последнего раунда расшифрования, что позволяет восстановить θ_1 и θ_2 . В результате получаем, что атака с внедрением ошибок позволяет восстановить ключ BelT-128 за 4 успешных внедрения ошибок.

Решением проблемы предложим два метода защиты аппаратных реализаций BelT [3]. Первый – временная избыточность, заключающаяся в выполнении каждой критической операции дважды, между вызовами которых вставляется случайная задержка, результаты которых сравниваются. Из-за случайной задержки нарушитель не может рассчитать точное время вызова. Второй – добавление битов четности к ключам и промежуточным значениям для обнаружения изменений. К каждому 32-разрядному ключевому слову добавляются 4 контрольных бита – по одному на каждый байт. Бит четности для байта вычисляется как XOR всех его битов. При каждой загрузке ключа устройство пересчитывает контрольные биты и сравнивает с сохраненными.

Заключение

Алгоритм BelT, являющийся стандартом Республики Беларусь, уязвим к атакам с внедрением ошибок. Для восстановления ключа достаточно 4 успешных внедрений ошибок. Уязвимость обусловлена отсутствием в стандарте требований к защите аппаратных реализаций от физических атак. При сертификации средств КЗИ на соответствие СТБ необходимо включать требования по защите от атак по сторонним каналам, включая атаки с внедрением ошибок.

Список использованных источников

1. СТБ 34.101.31-2020. (2020) *Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности*. Минск, Госстандарт.
2. Jovanovic P., Polian I. (2015) Fault-based Attacks on the Bel-T Block Cipher Family. *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 601-604.
3. Boneh D., DeMillo R., Lipton R. (2001) On the Importance of Elimination Errors in Cryptographic Computations. *Journal of Cryptology*. 14, 101–119.

References

1. STB 34.101.31-2020. (2020) *Information Technologies and Security. Algorithms for Encryption and Integrity Control*. Minsk, Gosstandart (in Russian).
2. Jovanovic P., Polian I. (2015) Fault-based Attacks on the Bel-T Block Cipher Family. *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 601-604.

3. Boneh D., DeMillo R., Lipton R. (2001) On the Importance of Elimination Errors in Cryptographic Computations. *Journal of Cryptology*. 14, 101–119.

Сведения об авторах

Герасимов А.С., магистр, старший преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.gerasimov@bsuir.by.

Макаренко К.Е., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», makarenkokirilka05@gmail.com.

Information about the authors

Gerasimov A.S., master, senior lecture, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.gerasimov@bsuir.by.

Makaranka K.E., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", makarenkokirilka05@gmail.com.

УДК 004.056.5

АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ

А.В. Шмавгонек

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассматриваются актуальные вопросы анализа уязвимостей и угроз информационной безопасности в корпоративных сетях. Особое внимание уделяется защите баз данных как ключевому элементу корпоративных информационных систем. Приведен анализ статистических данных по киберпреступности в Республике Беларусь за 2025 год, включая динамику финансовых потерь и структуру правонарушений. Обоснована необходимость регулярного проведения тестирования на проникновение (пентеста) как эффективного метода выявления недостатков защиты и прогнозирования экономических рисков.

Ключевые слова: информационная безопасность; корпоративная сеть; базы данных; уязвимости; угрозы; киберпреступность; тестирование на проникновение; пентест; анализ защищенности; экономические риски.

VULNERABILITY AND THREAT ANALYSIS IN CORPORATE NETWORKS

A.V. Shmavgonets

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The current issues of analyzing vulnerabilities and threats to information security in corporate networks are considered. Special attention is paid to database protection as a key element of corporate information systems. The analysis of statistical data on cybercrime in the

Republic of Belarus for 2025, including the dynamics of financial losses and the structure of offenses, is presented. The necessity of regular penetration testing (pentest) is substantiated as an effective method of identifying protection deficiencies and forecasting economic risks.

Keywords: information security; corporate network; databases; vulnerabilities; threats; cybercrime; penetration testing; pentest; security analysis; economic risks.

Введение

В современном мире информационные технологии играют ключевую роль в деятельности организаций и предприятий. Одним из важнейших компонентов корпоративных информационных систем являются базы данных, в которых аккумулируются сведения о клиентах, сотрудниках, финансовых операциях, партнерах, а также критически важная коммерческая информация.

Необходимость защиты информации в базах данных обусловлена также тем, что современные корпоративные системы тесно интегрированы с внешними сервисами, облачными решениями и сетевыми приложениями. Это значительно расширяет поверхность атаки и повышает вероятность компрометации данных.

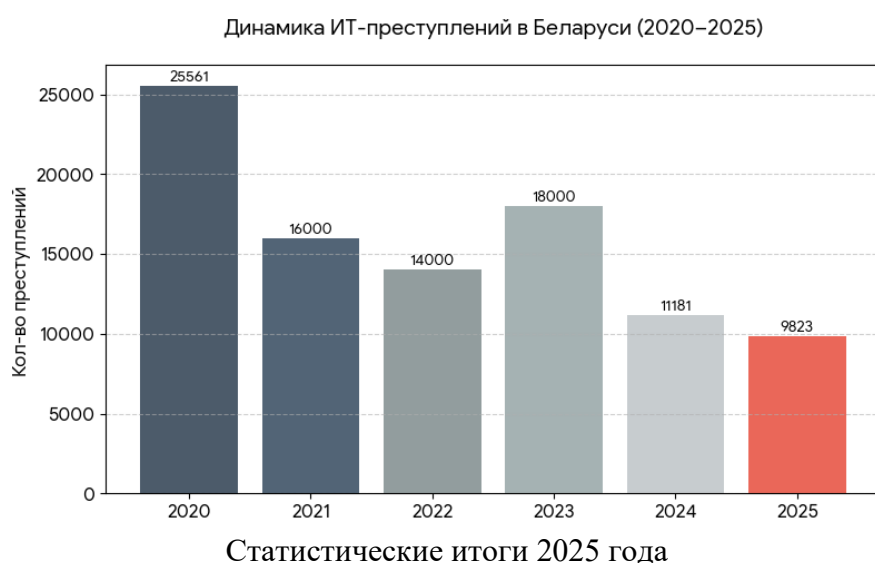
Актуальность темы определяется тем, что обеспечение информационной безопасности корпоративных баз данных является ключевым условием стабильной работы предприятия, непрерывности бизнеспроцессов и доверия клиентов.

Основная часть

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был невелик, так как зависимость мировой экономики от информационных технологий была мала. В настоящее время в условиях значительной зависимости бизнеса от электронных средств доступа и обмена информацией и постоянно растущего числа атак ущерб от самых незначительных атак, приводящих к потерям машинного времени, исчисляется миллионами долларов, а совокупный годовой ущерб мировой экономике составляет десятки миллиардов долларов.

Статистические итоги 2025 года в Республике Беларусь демонстрируют тревожные тенденции. Зарегистрировано снижение количества киберпреступлений на 6% (9 823 преступления), однако при этом наблюдается рост «качества» атак: финансовые потери граждан составили более 54 миллионов белорусских рублей. От действий преступников пострадали 19 тысяч человек, при этом около 96% всех киберпреступлений направлены на завладение денежными средствами. Средний чек кражи вырос с 2 500 BYN в 2024 году до 4 000+ BYN в 2025-м, участились случаи хищения сумм свыше 100–150 тысяч рублей.

Правоохранительными органами было выявлено и заблокировано почти 15 тысяч мошеннических интернет-ресурсов.



Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации, сосредоточение в базах данных информации различного уровня важности и конфиденциальности, расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети, увеличение числа удаленных рабочих мест, широкое использование глобальной сети Internet и различных каналов связи, автоматизация обмена информацией между компьютерами пользователей.

Корпоративная информационная система представляет собой сложную структуру, в которой объединены различные сервисы, необходимые для функционирования компании. Эта структура постоянно меняется – появляются новые элементы, изменяется конфигурация существующих. По мере роста системы обеспечение информационной безопасности и защита критически важных для бизнеса ресурсов становятся все более сложной задачей.

Для того чтобы выявить недостатки защиты различных компонентов и определить потенциальные векторы атак на информационные ресурсы, проводится анализ защищенности. Эффективный способ анализа – тестирование на проникновение (пентест), в ходе которого моделируется реальная атака злоумышленников. Цель тестирования – обнаружить возможные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу от обслуживания, а также спрогнозировать возможные финансовые потери и экономические риски.

Технологии информационной безопасности очень быстро устаревают, решение, оптимальное для предприятия заказчика на данный момент, не будет таковым через некоторое время. Поэтому многие специалисты по информационной безопасности рекомендуют проводить penetration test на регулярной основе, наилучшее решение – ежегодно.

Заключение

В результате проведенного анализа установлено, что корпоративные сети и базы данных в современных условиях подвергаются качественно новым угрозам. Интеграция с внешними сервисами расширяет поверхность атаки, делая традиционные методы защиты недостаточными. Статистика киберпреступлений в Беларуси за 2025 год подтверждает общемировой тренд: снижение количества атак сопровождается резким ростом их эффективности и финансовых потерь для жертв (средний чек превысил 4 000 BYN). Это свидетельствует о профессионализации киберпреступности и ее нацеленности на непосредственное хищение средств.

В сложившихся условиях ключевым инструментом обеспечения информационной безопасности становится регулярное тестирование на проникновение. Ежегодное проведение таких работ должно стать обязательной практикой для предприятий, стремящихся к сохранению непрерывности бизнес-процессов и защите критически важных данных.

Список использованных источников

1. Олифер В.Г., Олифер Н.А. (2007) Компьютерные сети. 2-ое изд. Москва, Вильямс.
2. Коллинз М. (2019) Защита сетей. Подход на основе анализа данных. Москва, ДМК.
3. Следственный комитет Республики Беларусь (2026) Официальные данные о состоянии киберпреступности в Республике Беларусь за 2025 год
4. Министерство внутренних дел Республики Беларусь (2026) Анализ финансовых потерь граждан от кибермошенников в 2024-2025 г.

References

1. Olifer V.G., Olifer N.A. (2007) Computer Networks. 2nd ed. Moscow, Williams Publishing House (in Russian).
2. Collins M. (2019) Network Security Through Data Analysis. Moscow, DMK Press (in Russian).
3. Investigative Committee of the Republic of Belarus (2026) Official Data on the State of Cybercrime in the Republic of Belarus for 2025 (in Russian).
4. Ministry of Internal Affairs of the Republic of Belarus (2026) Analysis of Citizens' Financial Losses from Cyber Fraud in 2024-2025 (in Russian).

Сведения об авторах

Шмавгонец А.В., магистрант факультета информационная безопасность. Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nastamoom2018@gmail.com

Information about the author

Shmavgonets A.V., Master's Degree Student, Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nastamoom2018@gmail.com

УДК 621.396

АНАЛИЗ ХАРАКТЕРИСТИК ТВЕРДОТЕЛЬНЫХ УСТРОЙСТВ В СВЧ ДИАПАЗОНЕ

И.В.Баженова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Возрастающие потребности человеческого общества в средствах передачи, приема и обработки информации привели к исключительно высоким темпам развития техники связи на сверхвысоких частотах (СВЧ) [1]. Этому способствовал прогресс в области развития полупроводниковой технологии, радиофизики и электроники сверхвысоких частот. В последние годы заметно усилилось развитие электронных СВЧ приборов, как вакуумных (клистронов, ЛБВ, магнетронов), так и полупроводниковых, последних – в особенности [2].

Ключевые слова: радиотехническая система, твердотельные устройства, виды модуляции, СВЧ диапазон, антенна, сигнал, длина волны, излучение, приемник, частота.

ANALYSIS OF THE CHARACTERISTICS OF SOLID-STATE DEVICES IN THE MICROWAVE RANGE

I.V. Bazhenova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The growing needs of human society for the means of transmitting, receiving, and processing information have led to exceptionally high rates of development in microwave communication technology [1]. This has been facilitated by progress in the development of semiconductor technology, radiophysics, and microwave electronics. In recent years, the development of microwave electronic devices, both vacuum (klystrons, TWTs, magnetrons) and semiconductor, particularly the latter, has noticeably accelerated [2].

Key words: radio engineering system, solid-state devices, types of modulation, microwave range, antenna, signal, wavelength, radiation, receiver, frequency.

Введение

Основой создания систем связи на СВЧ стали новые поколения приборов и устройств на твердом теле, выполняющие функции фильтрации, генерирования и усиления колебаний, стабилизации частоты, формирования и обработки сигналов [3]. Только на основе применения твердотельных устройств стали возможны: прием чрезвычайно слабых сигналов, микроминиатюризация, повышение надежности, КПД, скорости перестройки приемопередающей аппаратуры, увеличения ее пропускной способности, длительности автономной работы, снижение себестоимости серийного производства средств связи и расходов при их эксплуатации.

Основная часть

Целью данной работы является изучить уровень современного развития элементной базы электроники СВЧ, разработок активных и пассивных устройств приемопередающих радиотехнических систем, решить задачу проектирования и разработки СВЧ связного передатчика на основе применения достижений отечественной твердотельной электроники СВЧ, активных и пассивных двухполюсников (диодных структур лавинно-пролетных приборов, диодов с междолинным переходом – диодов Ганна, диодов с барьером Шоттки и т.д.), трехсантиметрового диапазона длин волн, как наиболее промышленно и технологически – освоенного диапазона.

Ценность диапазона СВЧ для систем связи определяется, прежде всего, широкополосностью и, следовательно, большой информационной емкостью. Широкополосность диапазона СВЧ позволяет применять помехоустойчивые частотную и фазовую модуляции, при которых уровень сигнала на выходе приемника в определенных пределах не зависит от уровня входного сигнала, изменяющегося вследствие замирания. Эти виды модуляции позволяют осуществлять высококачественную телефонную связь, вести трансляцию программ телевидения, передавать с большой скоростью без потерь достоверности цифровую информацию в сетях связи.

В диапазоне СВЧ сравнительно несложно создавать антенны с размерами, во много превышающими длину волны и обладающими воздействием этого остронаправленного излучения. Такие антенны позволяют осуществлять пространственную селекцию сигналов, обеспечивающую повышение помехозащищенности радиосистем и работу в заданном районе нескольких радиолиний с повторяющимися рабочими частотами без нарушения условий электромагнитной совместимости. Остронаправленное излучение повышает энергетический потенциал

радиолинии, разрешающую способность радиолокационного обнаружения и точность определения координат цели.

Заключение

Таким образом, развитие техники, совершенствование технологий электроники СВЧ, освоение с промышленных позиций диапазона СВЧ являются всегда приоритетными направлениями. Поэтому разработка твердотельных устройств и комплектов управляемых адаптивных систем, совершенствование СВЧ передатчиков и приемных блоков, несомненно, обладают новизной и относятся к разряду актуальных задач не только с точки зрения инженерной практики, но и для научно-исследовательской проработки вопросов по отдельным перспективам проблемных изысканий.

Список использованных источников

1. Лебедев И.В. Техника и приборы СВЧ, ч.2, 1972
2. Клич С.М. Проектирование СВЧ устройств радиолокационных приемников. М.: «Радио и связь», 1973, 320с.
3. Гасанов Л.Г. и др. Твердотельные устройства СВЧ в технике связи. М.: «Радио и связь» 1988, 288с.

References

1. Lebedev I.V. Microwave Technology and Devices, Part 2, 1972
2. Klich S.M. Design of Microwave Devices for Radar Receivers. Moscow: Radio and Communications, 1973, 320 pages.
3. Gasanov L.G. et al. Solid-State Microwave Devices in Communications Engineering. Moscow: Radio and Communications, 1988, 288 pages.

Сведения об авторах

Баженова И.В., канд. физ.-мат. наук, доцент, доцент кафедры «Вычислительные методы и программирование» Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», liv@bsuir.by.

Information about the authors

Bazhenova I.V., Ph.D. in Physics and Mathematics, Associate Professor, Associate Professor of the Department of Computational Methods and Programming of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", liv@bsuir.by.

УДК 621.396

ГЕНЕРАТОРЫ СВЧ С ВНЕШНЕЙ ДОПОЛНИТЕЛЬНОЙ ОБРАТНОЙ СВЯЗЬЮ

И.В.Баженова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Твердотельные электрически перестраиваемые генераторы находят все более широкое применение в различных радиотехнических устройствах [1]. В свою очередь требования к их параметрам определяются функциями, которые они должны выполнять в комплексе. Успешное применение генераторов на диодах Ганна в различных радиотехнических системах обусловлено возможностью их электрически перестраивать по частоте.

Ключевые слова: радиотехническая система, твердотельные устройства, виды модуляции, СВЧ диапазон, фазовращатель, генератор, фаза, обратная связь, варактор, частота.

MICROWAVE GENERATORS WITH EXTERNAL ADDITIONAL FEEDBACK

I.V. Bazhenova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. Solid-state electrically tunable oscillators are increasingly used in various electronic devices [1]. The requirements for their parameters, in turn, are determined by the functions they must perform together. The successful use of Gunn diode oscillators in various electronic systems is due to their ability to be electrically tunable in frequency.

Keywords: electronic system, solid-state devices, modulation types, microwave range, phase shifter, oscillator, phase, feedback, varactor, frequency.

Введение

В традиционных схемах генераторов сверхвысоких частот (СВЧ), работающих в автономном и синхронизированном режимах, для управления частотой и фазой используются варакторы [2]. Однако по ряду причин не во всех генераторах имеются встроенные в колебательную систему варакторы.

В таких генераторах управление частотой или фазой колебаний возможно осуществлением изменением модуля и фазы коэффициента передачи внешней дополнительной обратной связи, подключенной к генератору.

Основная часть

В автогенераторе СВЧ с внешней дополнительной обратной связью возможно осуществить автоматическую регулировку частоты, используя в качестве управителя частоты, электрически управляемые фазовращатель или аттенюатор в цепи внешней дополнительной обратной связи, напряжение на которые поступает с резистора в цепи питания генератора или с амплитудного детектора, включенного на выходе генератора СВЧ [3]. В результате анализа таких схем получены соотношения для коэффициента стабилизации частоты. Найдены оптимальные величины модуля и фазы коэффициента передачи цепи внешней дополнительной обратной связи, обеспечивающие снижение детерминированных уходов частоты в 10-20 раз.

Анализ искажений частотно модулированных сигналов, формируемых с помощью автогенераторов с внешней дополнительной обратной связью, показывает, что при подведении модулирующего напряжения к электрически управляемому фазовращателю в цепи с внешней дополнительной обратной связью или к питающему электроду выбором параметров цепи внешней дополнительной обратной связи возможно если снизить коэффициент нелинейных искажений по сравнению с генератором без внешней дополнительной обратной связи.

В синхронизированном генераторе с внешней дополнительной обратной связью можно реализовать ряд схем автоматической регулировки фазового набега путем подачи управляющего сигнала с резистора в цепи питания генератора или с фазового детектора на электрически управляемый фазовращатель в цепи внешней дополнительной обратной связи.

Заключение

Таким образом, проведенный анализ показал, что при определенных параметрах цепи с внешней дополнительной обратной связью величина фазового набега может быть снижена в несколько десятков раз.

Список использованных источников

1. Гасанов Л.Г. и др. Твердотельные устройства СВЧ в технике связи. М.: «Радио и связь», 1988, 288с.
2. Лебедев И.В. Техника и приборы СВЧ, ч.2, 1972.
3. Каганов В.И. СВЧ полупроводниковые передатчики. М.: «Радио и связь», 1981, 400с.

References

1. Gasanov L.G. et al. Solid-State Microwave Devices in Communication Engineering. Moscow: Radio and Communications, 1988, 288 pages.
2. Lebedev I.V. Microwave Technology and Devices, Part 2, 1972.
3. Kaganov V.I. Microwave Semiconductor Transmitters. Moscow: Radio and Communications, 1981, 400 pages.

Сведения об авторах

Баженова И.В., канд. физ.-мат. наук, доцент, доцент кафедры «Вычислительные методы и программирование» Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», liv@bsuir.by.

Information about the authors

Bazhenova I.V., Ph.D. in Physics and Mathematics, Associate Professor, Associate Professor of the Department of Computational Methods and Programming of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", liv@bsuir.by.

УДК 004.93'1

ПРОГНОЗИРОВАНИЕ ПОВЕДЕНИЯ ОБЪЕКТА С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ИНТЕЛЛЕКТУАЛЬНОГО ВИДЕОНАБЛЮДЕНИЯ

Р.В. Шерышев, Д. А. Коваленко, Ч. В. Ободо

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В работе рассматриваются современные системы интеллектуального видеонаблюдения, построенные на базе клиент-серверной архитектуры и методов компьютерного зрения. Особое внимание уделяется прогнозированию поведения объектов как расширенному функционалу видеоаналитики. Анализируются основные задачи: обнаружение, сопровождение, классификация и идентификация объектов, а также классификация видеоаналитики по сферам применения. Определены ключевые факторы, влияющие на эффективность прогнозирования, включая качество передачи данных и алгоритмическую проработку.

Ключевые слова: интеллектуальное видеонаблюдение; видеоаналитика; прогнозирование; поведение объектов; компьютерное зрение; обнаружение; распознавание; клиент-серверная архитектура; безопасность; алгоритмы.

PREDICTING OBJECT BEHAVIOR USING INTELLIGENT VIDEO SURVEILLANCE SYSTEMS

R.V. Sheryshev, D. A. Kavalenka, Ch. W. Obodo

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The paper considers modern intelligent video surveillance systems based on client-server architecture and computer vision methods. Particular attention is paid to predicting the behavior of objects as an advanced video analytics feature. The main tasks are analyzed: detection, tracking, classification and identification of objects, as well as classification of video analytics by application areas. Key factors influencing prediction effectiveness are identified, including data transmission quality and algorithmic elaboration.

Keywords: intelligent video surveillance; video analytics; forecasting; object behavior; computer vision; detection; recognition; client-server architecture; security; algorithms.

Введение

Современные системы видеонаблюдения, построенные на базе одной или нескольких видеокамер, обеспечивают непрерывный визуальный контроль заданных областей пространства. Цифровой формат видеоданных позволяет не только хранить и просматривать записи, но и применять специализированные технологии сжатия, поиска и передачи информации для оценки изменений наблюдаемой обстановки [1, 2]. Настоящая работа посвящена анализу возможностей прогнозирования поведения объектов, которое становится доступным благодаря внедрению интеллектуальных компонентов в системы видеонаблюдения.

Основная часть

Основой систем видеонаблюдения является клиент-серверная архитектура, когда информация от видеокамер передается по каналам связи на сервер, где можно производить видеоанализ (рисунок 1). Именно на серверной стороне применяются методы компьютерного зрения, позволяющие автоматизировать сбор данных на основе анализа видеоизображений. По результатам видеоаналитики выдаются сообщения об опасных объектах или нештатных событиях с последующей передачей этой информации оператору для принятия решений.

С помощью видеоаналитики реализуется комплекс задач, включающий обнаружение объектов посредством видеодетекторов движения, их сопровождение с использованием нескольких камер и специальных алгоритмов обработки, классификацию на основе формы и размеров, идентификацию, а также распознавание тревожных ситуаций путем анализа поведения объекта наблюдения. Расширенный функционал современных систем позволяет не только констатировать текущие события, но и прогнозировать дальнейшее поведение объекта, применять интеллектуальное сжатие видеоряда и ранжировать события по степени их приоритетности.

С практической точки зрения видеоаналитика подразделяется на несколько типов в зависимости от решаемых задач. Периметральная аналитика ориентирована на охрану протяженных участков и рубежей.

Ситуационная аналитика занимается распознаванием тревожных ситуаций, связанных с поведением людей. Биометрическая аналитика обеспечивает идентификацию личности по характерным признакам, а бизнес-аналитика служит инструментом управления организацией на основе собираемых данных.



Структурная схема системы интеллектуального видеонаблюдения
Structural diagram of the intelligent video surveillance system

Заключение

Проведенный анализ позволяет заключить, что эффективность работы устройств видеоаналитики определяется совокупностью факторов, среди которых ключевую роль играют качество каналов передачи информации, уровень алгоритмической проработки и особенности программной реализации. Для успешного функционирования систем распознавания необходима предварительная настройка видеоаналитики, причем высокое качество канала передачи данных создает условия для более эффективного обнаружения объектов и очистки изображения от шумов на начальных этапах обработки.

Список использованных источников

1. Ивашевский М. Р., Журавлева Л. М., Ефимова Н. О., Яцкивский Н. В. (2017) Оценка качества передачи сигналов систем интеллектуального видеонаблюдения. Проектирование и технология электронных средств. (3), 10–15.
2. Журавлева Л. М., Богачёв А. П., Яцкивский Н. В. (2017) Снижение аварийных рисков с помощью систем интеллектуального видеонаблюдения. Мир транспорта. (3), 206–212.

References

1. Ivashevskii M. R., Zhuravleva L. M., Efimova N. O., Yatskiivskii N. V. (2017) Evaluation of the Quality of Signal Transmission in Intelligent Video Surveillance Systems. Design and Technology of Electronic Means. (3), 10–15.
2. Zhuravleva L. M., Bogachev A. P., Yatskiivskii N. V. (2017) Reducing Accident Risks with the Help of Intelligent Video Surveillance Systems. World of Transport. (3), 206–212.

Сведения об авторах

Шерышев Р.В., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», romasheryshev@gmail.com.

Коваленко Д.А., инженер-химик НИЛ «Многофункциональные металлооксидные композитные материалы», учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kavalenka.d.a@gmail.com.

Ободо Ч.В., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», chidozieobodo13@gmail.com

Information about the authors

Sheryshev R.V., student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, romasheryshev@gmail.com.

Kavalenka D.A., chemical engineer of the Research Laboratory “Multifunctional Metal-Oxide. Composite Materials”, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, kavalenka.d.a@gmail.com.

Obodo Ch.W., master student information security department, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, chidozieobodo13@gmail.com.

УДК 621.382.323–027.45

СРАВНЕНИЕ ПО КРИТЕРИЯМ БАЙЕСА И НЕЙМАНА-ПИРСОНА МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ

С.М. Боровиков

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Приводится сравнение по критериям Байеса и Неймана-Пирсона моделей прогнозирования класса надежности изделий электронной техники для заданной наработки по значениям информативных параметров изделий в начальный момент времени. В качестве изделий электронной техники были выбраны полевые МОП-транзисторы большой мощности КП744А. Сравнение моделей прогнозирования выполнялось для разновидностей метода пороговой логики с преобразованием информативных параметров в двоичный и троичный коды. По результатам сравнения определена модель, рекомендуемая к использованию в практике.

Ключевые слова: изделия электронной техники, надежность, модели прогнозирования, прогнозирующая функция, критерии эффективности.

COMPARISON OF RELIABILITY PREDICTION MODELS FOR ELECTRONIC PRODUCTS WITH OF BAYESIAN AND NEYMAN-PEARSON CRITERIA

S.M. Borovikov

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The article presents a comparison by Bayesian and Neyman-Pearson criteria for models of predicting the reliability class of electronic products for a given operating time based on the values of informative parameters of products at the initial point in time. High-power MOS field-effect transistors (KP744A) were selected as the electronic products. The prediction models were compared for variations of the threshold logic method with using the transformation of informative parameters into binary and ternary codes. Based on the comparison results, a model recommended for practical use was determined.

Keywords: Electronic products, reliability, prediction models, prediction function, performance criteria.

Введение

В применении к индивидуальному прогнозированию класса надежности изделий электронной техники (ИЭТ) для заданной наработки критерий Байеса используют в двух разновидностях [1]:

а) $P_{\text{прав}} \rightarrow \max$, (1)

где $P_{\text{прав}}$ – вероятность принятия правильных решений (распознаваний) класса надежности экземпляров ИЭТ для заданной (будущей) наработки:

класс надежных экземпляров (K_1), класс потенциально ненадежных экземпляров (K_2);

$$\text{б) } \rho \rightarrow \min, \quad (2)$$

где ρ – средние удельные потери из-за возможного наличия при прогнозировании ошибок первого рода $n_{1 \rightarrow 2}$, состоящих в том, что в действительности надежный для заданной наработки экземпляр (класс K_1) по прогнозу будет рассматриваться как потенциально ненадежный (класс K_2), и ошибок второго рода $n_{2 \rightarrow 1}$, состоящих в том, что в действительности потенциально ненадежный для заданной наработки экземпляр (класс K_2) по прогнозу будет признан надежным (класс K_1).

Согласно работе [1], выражение для определения потерь ρ примет вид

$$\rho = [1 - P(K_1)] \cdot P_1 \cdot C_{12} + [1 - P(K_2)] \cdot P_2 \cdot C_{21} \rightarrow \min, \quad (3)$$

где $P(K_1)$, $P(K_2)$ – вероятность правильного распознавания (при прогнозировании) соответственно экземпляров классов надежности K_1 и K_2 ; P_1 , P_2 – определяемые по результатам обучающего эксперимента начальные (априорные) вероятности принадлежности прогнозируемого экземпляра для заданной наработки соответственно к классам надежности K_1 и K_2 ; C_{12} , C_{21} – средняя удельная цена потерь, обусловленная соответственно ошибками первого $n_{1 \rightarrow 2}$ и второго $n_{2 \rightarrow 1}$ рода.

Критерий Неймана-Пирсона с позиций изготовителей электронных устройств, являющимися потребителями ИЭТ, будем использовать в виде [2]

$$P_{\text{изг}} \rightarrow \min \text{ при } P_{\text{потр}} \leq P_{\text{потр.доп}}, \quad (4)$$

где $P_{\text{изг}}$, $P_{\text{потр}}$ – риски изготовителя и потребителя, показывают возможную долю соответственно ошибок первого $n_{1 \rightarrow 2}$ и второго $n_{2 \rightarrow 1}$ рода в прогнозируемой выборке ИЭТ; $P_{\text{потр.доп}}$ – допустимое значение риска потребителя, выбранное для задачи индивидуального прогнозирования.

Основная часть

В работе исследованы следующие модели прогнозирования, применяемые к выборке ИЭТ – полевым МОП транзисторам КП744А:

1. Модель прогнозирования, получаемая базовым методом пороговой логики [1, 2] по результатам преобразования информативных параметров в двоичный код (ноль или единица). Здесь прогнозирующая функция $F^{(j)}$ конкретного (j -го) экземпляра показывает его близость к классу надежности K_1 .

2. Аналог модели прогнозирования базового метода пороговой логики, но получаемой с учетом преобразования информативных параметров в троичный код (1, 0 или R – неопределенность) [3], где R – код, присваиваемый в случае, если для прогнозируемого экземпляра

информативный параметр попадает в диапазон между его средними значениями, соответствующими экземплярам классов надежности K_1 и K_2 для экземпляров обучающей выборки. Прогнозирующая функция $F^{(j)}$ для этой модели представляет собой показатель близости прогнозируемого экземпляра к классу надежности K_1 .

3. Модель, использующая преобразование информативных параметров в троичный код (1, 0 и R) [3], но прогнозирующая функция $F^{(j)}$ представляет собой разность между показателями близости прогнозируемого экземпляра к классам надежности K_1 и K_2 .

Результаты сравнения описанных моделей приведены в таблице.

Сравнение моделей прогнозирования по критериям Байеса и Неймана-Пирсона
Comparison of forecasting models using Bayes and Neyman-Pearson criteria

Модель (пункт)	Критерий Байеса		Критерий Неймана-Пирсона: $P_{\text{изг}} (\%)$ при $P_{\text{потр. доп}} \leq 2 \%$
	$P_{\text{прав}} \rightarrow \max$	$\rho \rightarrow \min$ в усл. ед. при $C_{12}: C_{21} = 1 : 100$	
1	0,878	9,92	23,5
2	0,901	4,70	16,3
3	0,901	4,12	12,5

Заключение

Из трех рассмотренных моделей лучшие результаты прогнозирования класса надежности ИЭТ для заданных (будущих) наработок обеспечивает модель прогнозирования, основанная на преобразовании информативных параметров в троичный код с построением прогнозирующей функции $F^{(j)}$ в виде разности между показателями близости прогнозируемого экземпляра к классам надежности K_1 и K_2 . Эта модель рекомендуется к применению в практике, теоретический порог разделения классов надежности в данном случае равен нулю.

Список использованных источников

1. Боровиков С.М. (2013) *Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники*. Москва, Издательство «Новое знание».
2. Боровиков С.М. (1998) *Теоретические основы проектирования, технологии и надежности*. Минск, Издательство «ДизайнПРО».
3. Казючиц В.О., Боровиков С.М., Батура М.П., Шнейдеров Е.Н. (2023) Прогнозирование класса надежности изделий электронной техники методом преобразования информативных параметров в дискретный код. *Доклады ТУСУР*. 26(1), 91–97.

References

1. Borovikov S.M. (2013) *Statistical Forecasting for Rejection of Potentially Unreliable Electronic Products*. Moscow, New Knowledge Publishing House (in Russian).

2. Borovikov S.M. (1998) *Theoretical foundations of design, technology and reliability*. Minsk, DesignPRO Publishing House (in Russian).

3. Kaziuchyts V.O., Borovikov S.M., Batura M.P., Shneiderov E.N. (2023) Prediction of the class of reliability of electronic equipment by the method of converting informative parameters into a discrete code. *TUSUR reports*. 26(1), 91–97 (in Russian).

Сведения об авторе

Боровиков С.М., канд. техн. наук, доц., доцент кафедры проектирования информационно-компьютерных систем, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bsm@bsuir.by.

Information about the author

Borovikov S., Cand. Sci. (Tech.), Associate professor of the Department of Information and Computer Systems Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", bsm@bsuir.by.

УДК 621.314.211 : 621.3.019.3

ОЦЕНКА НАДЕЖНОСТИ ИМПУЛЬСНЫХ ТРАНСФОРМАТОРОВ С УЧЕТОМ ИХ КОНСТРУКТИВНЫХ ОСОБЕННОСТЕЙ

С.М. Боровиков¹, Е.Д. Гришечкин¹, А.В. Будник²

¹ Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

² Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь

Аннотация. Рассматривается расчет надежности импульсных трансформаторов с учетом их конструктивных параметров и тепловых потерь в проводах обмоток и ферритовом сердечнике на примере трансформатора строчной развертки телевизионного приемника. Установлено, что учет этих факторов обеспечивает расчетные показатели надежности, которые лучше подтверждаются экспериментальными данными, нежели результаты, полученные с использованием классических методик, основанных на использовании только поправочных коэффициентов для интенсивности отказов трансформаторов.

Ключевые слова: импульсные трансформаторы; эксплуатационная надежность; интенсивность отказов; прогнозирование надежности; учет конструктивных параметров.

RELIABILITY ASSESSMENT OF PULSE TRANSFORMERS WITH CONSIDERATION OF THEIR DESIGN FEATURES

S.M. Borovikov¹, E.D. Grieshechkin¹, A.V. Budnik²

¹ Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus

² Educational Institution "Belarusian State Academy of Communications",
Minsk, Republic of Belarus

Abstract. This paper examines the reliability calculations for pulse transformers, taking into account their design parameters and thermal losses in the winding wires and ferrite core, using the example of a horizontal-scan transformer for a television receiver. It is established that taking these factors into account provides calculated reliability indicators that are better supported by experimental data than results obtained using classical methods based on only using correction factors for failure rate of transformer.

Keywords: pulse transformers, operational reliability, failure rate; reliability prediction; consideration of design parameters.

Введение

В работе представлены результаты оценки эксплуатационной интенсивности отказов импульсного трансформатора с учетом его конструктивных особенностей (геометрических размеров, количества обмоток и диаметра используемых проводов, количества внешних выводов), а также тепловых потерь в обмоточных проводах и ферритовом сердечнике. Результаты приведены применительно к трансформатору строчной развертки ТВС-110ПЦ16, для которого были найдены данные о надежности из опыта эксплуатации. Конструктивно этот тип трансформатора представляет собой стержневой ферритовый магнитопровод, на котором размещается гильза из изоляционного материала с девятью обмотками. Сечение стержня магнитопровода: ширина $a = 10$ мм, толщина $b = 7,5$ мм. Ширина c и высота h окна для размещения обмоток: $c = 15$ мм и $h = 23$ мм. Диаметр проводов (от 0,14 мм до 0,4 мм) и количество витков (от 4 до 1050) приведены в [1].

Основная часть

В качестве показателя надежности импульсного трансформатора рассматривается эксплуатационная интенсивность отказов $\lambda_{\text{экс}}$. Для прогнозирования $\lambda_{\text{экс}}$ использована предложенная авторами модель

$$\lambda_{\text{экс}} = \left(K_T \cdot K_{\text{Э.пр}} \cdot K_{\text{П.пр}} \sum_i^n \lambda_{\text{пр}i} K_{di} L_i + 2K_t \cdot K_{\text{Э.к}} \cdot K_{\text{П.к}} \sum_i^n \lambda_{\text{к}i} K_{di} \right) K_{\text{Э}} \cdot K_{\text{П}}, \quad (1)$$

где K_T – коэффициент, учитывающий влияние температуры на надежность изоляции проводов [3]; n – общее число обмоток в трансформаторе;

$\lambda_{\text{при}}$ – базовая интенсивность отказов 2-ой обмоточного провода i -й обмотки; K_{di} – поправочный коэффициент, учитывающий диаметр обмоточного провода i -й обмотки; $\lambda_{\text{ки}}$ – базовая интенсивность отказов паяных соединений выводов обмоток к внешним контактам трансформатора; K_t – поправочный коэффициент, учитывающий влияние температуры на интенсивность отказов паяных соединений; $K_{\text{Э.пр}}$, $K_{\text{Э.к}}$, $K_{\text{Э}}$, $K_{\text{П.пр}}$, $K_{\text{П.к}}$, $K_{\text{П}}$ – коэффициенты эксплуатации (Э) и приемки (П), соответствующие обмоточным проводам (пр), паяным контактными соединениями (К) и трансформатору в целом.

Принимая во внимание геометрические размеры магнитопровода и особенность каркаса из изоляционного материала, используемого для намотки трансформатора, определена длина провода обмоток. По диаметру и длине проводов было рассчитано сопротивление провода для каждой обмотки и с учетом протекающих в обмотках токов определены суммарные потери в медных проводах трансформатора ($P_{\text{кз}}$). Для оценки потерь в сердечнике использованы характеристики феррита и рабочая частота трансформатора $f = 15,6$ кГц. С учетом удельных потерь в феррите магнитопровода ($P_{\text{уд}}$) и массы сердечника магнитопровода M_c найдена мощность потерь в сердечнике P_c и далее определена суммарная мощность тепловых потерь P_{Σ} .

По геометрическим размерам магнитопровода и каркаса, используемого для намотки проводов, с учетом обеспечения технологических зазоров рассчитана площадь охлаждающей поверхности трансформатора ($S_{\text{охл}}$). По эмпирической формуле, приводимой в [2] для трансформаторов, используя полученные значения P_{Σ} и $S_{\text{охл}}$, определена температура перегрева трансформатора $t_{\text{п}}$. Температура окружающей среды $T_{\text{окр}}$ для обмоток трансформатора с учетом рабочей температуры электронного устройства $T_{\text{ЭУ}}$ принята равной $T_{\text{окр}} = T_{\text{ЭУ}} + t_{\text{п}}$.

В таблице приведены расчетные данные, полученные для рассматриваемого импульсного трансформатора ТВС-110ПЦ16.

Расчетные параметры для импульсного трансформатора
Calculation parameters for a pulse transformer

Параметр	Значение	Параметр	Значение	Параметр	Значение
$P_{\text{кз}}$, Вт	0,254	P_c , Вт	1,11	$t_{\text{п}}$, °C	41,9
$P_{\text{уд}}$, Вт/кг	17,72	P_{Σ} , Вт	1,364	$T_{\text{ЭУ}}$, °C	40
M_c , кг	0,062	$S_{\text{охл}}$, см ²	26,67	$T_{\text{окр}}$, °C	≈ 82

Полученные значения эксплуатационной интенсивности отказов $\lambda_{\text{экс}}$ импульсного трансформатора: а) прогнозированием по модели (1), $\lambda_{\text{экс}} = 1,19 \cdot 10^{-6}$ 1/ч; б) прогнозированием по модели справочника [3], $\lambda_{\text{экс}} = 0,00973 \cdot 10^{-6}$ 1/ч; в) из опыта эксплуатации, $\lambda_{\text{экс}} = 1,0 \cdot 10^{-6}$ 1/ч.

Заключение

Учет используемых материалов и конструктивных параметров трансформатора, его функциональной структуры (количества обмоток, типа и диаметров используемых обмоточных проводов) и рабочей частоты на примере импульсного трансформатора ТВС-110ПЦ16 позволил получить расчетное значение эксплуатационного показателя надежности (эксплуатационной интенсивности отказов) значительно лучше подтверждающееся данными из опыта эксплуатации трансформаторов этого типа в составе электронных устройств.

Список использованных источников

1. Громов Н.В. (1987) Телевизоры цветного изображения: справочная книга. Ленинград, Издательство «Лениздат».
2. A universal model for reliability prediction of Electronics components, PCBs and equipment. RDF 2000: reliability data handbook (2000). – Paris, UTE C 80-810.
3. Прытков С.Ф., Горбачева В. М., Борисов А. А. (2008) Надежность электрорадиоизделий: справочник. Москва, ФГУП «22 ЦНИИ МО РФ».

References

1. Gromov N.V. (1987) Color Televisions: Reference Book Leningrad, Lenizdat Publishing (in Russian).
2. A universal model for reliability prediction of Electronics components, PCBs and equipment. RDF 2000: reliability data handbook (2000). – Paris, UTE C 80-810.
3. Prytkov S.F., Gorbacheva V. M., Borisov A. A. (2008) Reliability of Electronic and Radio Components: Reference Book. Moscow, FSUE "22 Central Research Institute of the Ministry of Defense of the Russian Federation" (in Russian).

Сведения об авторах

Боровиков С.М., канд. техн. наук, доц., доц. каф. ПИКС, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bsm@bsuir.by.

Гришечкин Е.Д., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», egorgr2977@gmail.com.

Будник А.В., канд. техн. наук, доц., декан факультета инжиниринга и технологий, учреждение образования «Белорусская государственная академия связи», A.Budnik@bsac.by.

Information about the authors

Borovikov S., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of ICSD, Educational Institution "Belarusian State University of Informatics and Radioelectronics", bsm@bsuir.by.

Grishechkin E., Master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", egorgr2977@gmail.com.

Budnik A., Cand. Sci. (Tech.), Associate Professor, Dean of the Faculty of Engineering and Technology, Educational Institution "Belarusian State Academy of Telecommunications", A.Budnik@bsac.by.

УДК 004.021

ПРИМЕРЫ ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ В WORDPRESS

Р.Д. Осипов, А.Ю. Савицкий, А.А. Игнатенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В 2025 – 2026 году популярность WordPress делает данную платформу приоритетной целью для кибератак. В статье анализируются актуальные угрозы безопасности, в частности SQL-инъекции. Рассматриваются риски, связанные с использованием кода, созданного искусственным интеллектом без аудита безопасности. Оценивается вероятность эксплуатации брешей в современной экосистеме WordPress и подчеркивается критическая важность защиты данных в условиях открытой архитектуры платформы.

Ключевые слова: WordPress; кибербезопасность; SQL-инъекции; A03:2021 – Injection; шаблон; уязвимости; искусственный интеллект; защита данных; веб-разработка; аудит безопасности.

EXAMPLES OF SQL INJECTION PROTECTION IN WORDPRESS

R.D. Osipov, A.Yu. Savitsky, A.A. Ignatenko

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. In 2025–2026, the popularity of WordPress makes the platform a primary target for cyberattacks. This article analyzes current security threats, specifically focusing on SQL injections. It examines the risks associated with using AI-generated code without a proper security audit. The study evaluates the probability of exploiting vulnerabilities within the modern WordPress ecosystem and emphasizes the critical importance of data protection given the platform's open architecture.

Keywords: WordPress; cybersecurity; SQL injection; A03:2021 – Injection; template; vulnerabilities; artificial intelligence; data protection; web development; security audit.

Введение

В 2025 – 2026 году WordPress продолжает доминировать на рынке веб-разработки обеспечивая работу более 43% всех сайтов в интернете [2]. Однако такая популярность имеет обратную сторону – огромная

экосистема становится главной мишенью для атакующих. По данным HackerOne и Pathstack, SQL-инъекции стабильно входят в число самых опасных угроз, составляя до 15% от всех выявленных уязвимостей в этой среде [2]. Несмотря на высокий уровень безопасности самого ядра WordPress, его открытая архитектура и массовое использование кода, созданного искусственным интеллектом без должного аудита, создают огромную поверхность для атак. Вероятность эксплуатации подобных брешей оценивается экспертами в 8,5 баллов из 10, что делает вопрос защиты данных приоритетным для любого владельца сайта [2].

Основная часть

Ключевой риск в современной веб-разработке классифицируется международном стандарте OWASP как категория A03:2021 – Injection. Данная угроза сохраняет свою критическую актуальность и в 2026 году [1]. Рассматриваемая проблема напрямую связана с классической ошибкой CWE-89, при которой стирается граница между программной логикой и данными пользователя, что позволяет злоумышленнику «подмешивать» собственные команды в запросы к базе данных.

Основные проблемы безопасности в WordPress обычно скрыты не в самом «движке», а в коде сторонних тем и плагинов. Чаще всего это происходит из-за того, что разработчики пренебрегают правильной проверкой входящих данных. Самый опасный сценарий – когда необработанная информация из адресной строки браузера или полей формы попадает напрямую в SQL-запрос. В современном мире нарушители используют высокоскоростные сканеры, которые за секунды находят такие ошибки и позволяют мгновенно менять структуру запросов, открывая доступ к конфиденциальной информации сайта.

Рассмотрим простой пример того, как выглядит опасный код, написанный на php[3]:

```
$id = $_GET['data_id'];  
$wpdb->query("DELETE FROM {$wpdb->prefix}data WHERE id = $id");
```

В данном случае нарушитель может передать вместо обычного номера команду – 123 OR 1=1. Это заставит базу данных выполнить команду для всех строк сразу, что приведет к удалению всех данных. Чтобы этого не случилось, в руководстве WordPress Developer Resources есть главный инструмент защиты – метод \$wpdb->prepare(). Он работает как шаблон: сначала пользователь пишет текст запроса с «метками», а потом передает данные. Система сама очистит их и подставит на нужные места, не давая нарушителю шансов изменить логику [1].

```
$id = $_GET[data_id'];  
$wpdb->query($wpdb->prepare(  
    "DELETE FROM {$wpdb->prefix}data WHERE id = $d",  
    $id  
));
```

Одной только подготовки запроса мало. Важно использовать «очистку» данных сразу, как только они поступили на сайт. Например, если пользователь ждет число, используйте функцию `absint()`, которая превратит любой странный текст в обычную цифру [2]. Огромную роль играют Nonces – это специальные проверочные ключи WordPress. Данные ключи подтверждают, что запрос отправил именно настоящий пользователь с сайта, а не посторонний скрипт со стороны [3].

```
if (! isset($_POST['my_nonce']) || ! wp_verify_nonce($_POST['my_nonce'],  
'delete_action' )){  
    wp_die('Текст который будет отображаться в случае ошибки');  
}
```

Заключение

Глубокое понимание механизмов работы инъекций в сочетании с регулярным сканированием системы – единственный надежный способ защитить проект сегодня. Безопасность WordPress – это непрерывный процесс, когда разработчик фильтрует каждое входящее слово, использует подготовленные запросы и применяет современные средства мониторинга, сайт остается по-настоящему защищенным от угроз категории A03:2021.

В современных условиях, когда атаки автоматизированы и происходят за доли секунды, уже нельзя полагаться на внимательность специалистов по информационной безопасности или базовые настройки сервера. Для обеспечения реальной безопасности сайта необходимо внедрять комплексную систему контроля, работающую на опережение. Консольный интерфейс WP-CLI позволяет разработчикам не только управлять контентом, но и оперативно проводить технический аудит, выявляя подозрительные изменения в файловой структуре. В то же время интеграция с специализированными базами данных, такими как WPScan и Patchstack, превращает защиту из пассивной в проактивную, где владельцы получают оповещения о критических уязвимостях в плагинах еще до того, как нарушители успеют ими воспользоваться.

Важно осознать, что безопасность WordPress – это не конечная точка, а непрерывный процесс. Только когда специалист по информационной безопасности фильтрует каждое входящее слово, строго использует параметризованные запросы `$wpdb->prepare()`

и применяет современные средства мониторинга в реальном времени, сайт остается по-настоящему защищенным. Во время ИИ-угроз многоуровневая оборона позволяет эффективно противостоять рискам категории A03:2021 – Injection, сохраняя репутацию проекта и конфиденциальность данных пользователей.

Список использованных источников

1. Атаки на веб и WordPress. – СПб.: БХВ-Петербург, 2021. – 256 с.
2. OWASP Top 10: [отчет] / OWASP Foundation. – 2021. – URL: owasp.org (дата обращения: 17.03.2026).
3. WordPress с нуля. – СПб.: БХВ-Петербург, 2021. – 304 с.

References

1. Attacks on Web and WordPress. St. Petersburg: BHV-Petersburg. 2021. 256 pages.
2. OWASP Top 10: [Report] / OWASP Foundation. 2021. URL: owasp.org (Accessed: 17.03.2026).
3. WordPress from Scratch. St. Petersburg: BHV-Petersburg 2021. 304 pages.

Сведения об авторах

Осипов Р.Д., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», osipovr695@gmail.com.

Савицкий А.Ю., кандидат военных наук, старший преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.savitskij@bsuir.by.

Игнатенко А.А., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.ignatenko@bsuir.by

Information about the authors

Osipov R.D., Cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, osipovr695@gmail.com.

Savitsky A.Yu., PhD in Military Science, Senior Lecturer, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.savitskij@bsuir.by.

Ignatenko A.A., Lecturer, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.ignatenko@bsuir.by.

УДК 004.056

ПОСТКВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ СТОЙКОСТИ ШИФРОВ

М.А. Солонович, А.А. Игнатенко

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В данной статье рассмотрены угрозы классическим криптографическим алгоритмам, которые представляют квантовые компьютеры. Обсуждаются симметричное и асимметричное шифрование. Описание алгоритмов Шора и Гровера. Использование искусственного интеллекта в повышении стойкости шифров: автоматизированный криптоанализ решеток и кодов, оптимизация параметров и генерация новых схем.

Ключевые слова: Криптография; квантовые компьютеры; постквантовые алгоритмы; алгоритм Шора; алгоритм Гровера; RSA; симметричное шифрование; асимметричное шифрование; искусственный интеллект; криптоанализ.

POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS AND THE APPLICATION OF ARTIFICIAL INTELLIGENCE TO ENHANCE THE STRENGTH OF CIPHERS

M.A. Solonovich, A.A. Ignatenko

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. This article examines the threats to classical cryptographic algorithms posed by quantum computers. Symmetric and asymmetric encryption are discussed. Shor's and Grover's algorithms are described. The use of artificial intelligence in increasing the security of ciphers: automated cryptanalysis of lattices and codes, parameter optimization, and the generation of new schemes.

Keywords: Cryptography; quantum computers; post-quantum algorithms; Shor's algorithm; Grover's algorithm; RSA; symmetric encryption; asymmetric encryption; artificial intelligence; cryptanalysis.

Введение

Криптография — это наука о защите информации путем преобразования исходных данных в шифр, обеспечивая конфиденциальность, целостность и аутентичность. Появление квантовых компьютеров создает угрозу классическим алгоритмам криптографии, основанным на факторизации числа и дискретном логарифмировании. Параллельно развитие искусственного интеллекта предоставляет как инструменты для атак, так и средства для проектирования стойких

постквантовых схем. Рассматриваются постквантовые криптографические алгоритмы и роль искусственного интеллекта в их разработке.

Основная часть

Криптография – это наука о защите информации путем преобразования исходных данных в шифр, обеспечивая конфиденциальность, целостность и аутентичность. В общем случае криптографическое преобразование позволяет преобразовать открытый текст в шифротекст при помощи некоторого алгоритма и секретного ключа.

Симметричный алгоритм шифрования – для шифровки и расшифровки используется одинаковый ключ.

Асимметричный алгоритм шифрования – для шифровки и расшифровки используются разные ключи: открытый ключ для шифрования, закрытый ключ для дешифровки.

В настоящее время криптография опирается на вычислительную сложность решения подбора ключей для расшифровки. Безопасность большинства асимметричных алгоритмов строится на том, что операции по созданию ключа выполнить легко, а для подбора ключа это будет крайне сложная задача. Например, произведение двух больших простых чисел p и q требует полиномиального времени, в то время как факторизация результирующего модуля имеет экспоненциальную сложность. На этой идее строится алгоритм шифрования RSA.

RSA относится к асимметричным алгоритмам шифрования, для шифрования информации используется открытый ключ, а для дешифровки используется закрытый ключ.

Вся безопасность данного алгоритма опирается на вычислительную сложность. Задача стоит только в том, чтобы разложить большое произведение на простые множители. И эта сложность актуальна только для обычных компьютеров.

Однако квантовые компьютеры при применении своих алгоритмов способны кардинально изменить ситуацию. Одним из них является Алгоритм Шора предназначен для факторизации целых чисел, позволяющий разложить число n на простые множители за $O(\log^3 n)$ операций, используя $O(\log n)$ кубитов.

Для атаки на симметричную криптографию используют алгоритм Гровера. В исходной постановке он позволяет отыскать в неупорядоченном списке из N элементов присутствующий в единственном экземпляре элемент с отличительным свойством за $O(\sqrt{N})$ шагов – итераций Гровера. Алгоритм Гровера может быть использован для ускорения атаки полным перебором.

В настоящее время на международном уровне ведется стандартизация постквантовых алгоритмов на решетках (Kyber), кодах (McEliece), хэшах (SPHINCS+), устойчивых к Шору/Гроверу. Злоумышленники уже реализуют стратегию «собери сейчас – расшифруй потом», накапливая зашифрованные данные для будущих квантовых атак.

На этом фоне особое значение приобретает применение методов искусственного интеллекта в постквантовой криптографии. Искусственный интеллект сильно ускоряет развитие постквантовой криптографии, беря на себя решение задач, ранее требовавших десятилетий ручного труда.

Нейронные сети анализируют сложные структуры решеток LWE и кодов McEliece, мгновенно выявляя критические уязвимости – короткие векторы или эквивалентные коды, на поиск которых у экспертов уходили месяцы. методы машинного обучения оптимизируют параметры алгоритмов. Генетические алгоритмы и градиентный спуск подбирают оптимальные значения q и β для Kyber и NTRU, обеспечивая минимальный размер ключей при сохранении требуемой стойкости против квантовых атак. Эволюционные алгоритмы и генеративно-сопоставительные сети (GAN) создают и тестируют модификации SPHINCS+ и Ring-LWE, автоматически проверяя устойчивость к алгоритмам Шора и Гровера.

Заключение

Существующие сегодня и повсеместно применяемые асимметричные алгоритмы уязвимы к квантовым атакам. Стоит отметить, что симметричные остаются частично стойкими при условии увеличения длины ключа. Постквантовая криптография предлагает новые математические основы. Искусственный интеллект полезен в постквантовой криптографии: он помогает автоматизировать и улучшать разработку постквантовых алгоритмов.

Список использованных источников

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.
2. Малыгина Е. С., Куценко А. В., Новоселов С. А., Колесников Н. С., Бахарев А. О., Хильчук И. С., Шапоренко А. С., Токарева Н. Н. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решетках // Дискретный анализ и исследование операций. – 2023. – Т. 30, № 4. – С. 46–90. – DOI: 10.33048/daio.2023.30.771.

References

1. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. *Osnovy kriptografii* [Fundamentals of cryptography]. 2nd ed. Moscow: Gelios ARV, 2002. 480 p. (In Russ.).
2. Malygina E. S., Kutsenko A. V., Novoselov S. A., Kolesnikov N. S., Bakharev A. O., Khilchuk I. S., Shaporenko A. S., Tokareva N. N. Post-quantum cryptosystems: open questions and existing solutions. Lattice-based cryptosystems. *Diskretnyi analiz i issledovanie operatsii* [Discrete Analysis and Operations Research], 2023, vol. 30, no. 4, pp. 46-90. (In Russ.) DOI: 10.33048/daio.2023.30.771.

Сведения об авторах

Солонович М.А., курсант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», maxnest77max@icloud.com.

Игнатенко А.А. магистр, преподаватель, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.ignatenko@bsuir.by.

Information about the authors

Solonovich M.A., Cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, maxnest77max@icloud.com.

Ignatenko A.A., Master, lecturer, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.ignatenko@bsuir.by.

УДК 004.056.53:004.8

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В SIEM ДЛЯ МИНИМИЗАЦИИ ОГРАНИЧЕНИЙ ПРАВИЛ КОРРЕЛЯЦИИ

Г.А. Славинский, В.А. Быстрова, Н.Л. Боброва

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье исследуется развитие SIEM-систем под влиянием технологий искусственного интеллекта. Систематизированы ключевые ограничения правил корреляции и проведен анализ возможностей современных интеллектуальных инструментов для их преодоления. Определены преимущества и недостатки подобной интеграции, выдвинуто предположение о будущем SIEM.

Ключевые слова: информационная безопасность; мониторинг событий; SIEM; искусственный интеллект; машинное обучение.

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN SIEM TO MINIMISE THE LIMITATIONS OF CORRELATION RULES

G.A. Slavinsky, V.A. Bystrova, N.L. Bobrova

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The article examines the evolution of SIEM systems under the influence of Artificial Intelligence technologies. It categorises the key limitations of correlation rules and analyses how modern AI-enhanced tools can overcome them. The study identifies the advantages and disadvantages of such integration and offers a perspective on the future of SIEM.

Keywords: information security; event monitoring; SIEM; artificial intelligence; machine learning.

Введение

SIEM – это решение для управления информацией и событиями безопасности, обеспечивающее централизованный сбор, нормализацию, корреляцию и анализ данных из множества источников инфраструктуры [1]. Его основная задача – формирование перечня инцидентов.

Решения класса SIEM можно классифицировать по архитектуре, модели поставки и функциональным возможностям [2]. В контексте данной статьи, ключевым критерием является метод выявления угроз: от использования заданных правил к адаптивным механизмам на базе технологий искусственного интеллекта. Существенные различия между этими подходами определяют их применимость в условиях роста сложности атак, что подчеркивает актуальность проводимого исследования.

Основная часть

Правила корреляции представляют собой набор условий для автоматического анализа событий и выявления признаков уже известных атак, их эффективность зависит от полноты и актуальности базы правил, что приводит к ряду существенных ограничений:

избыточный объем данных, высокая доля ложноположительных срабатываний;

неспособность обнаружения новых угроз из-за отсутствия известных шаблонов поведения;

проблема выявления сложных атак на основе последовательности событий, распределенных во времени и по их источникам;

необходимость экспертизы со стороны опытного аналитика для быстрого расследования инцидента.

Указанные ограничения являются основанием для внедрения перспективных технологий – искусственного интеллекта (ИИ), способного повысить эффективность обнаружения угроз [3]. Среди ключевых возможностей ИИ: извлечение знаний и закономерностей из больших объемов данных, выявление скрытых паттернов, автоматизация бизнес-логики.

Эволюция SIEM предполагает переход к новым архитектурным решениям. Основой автоматизации бизнес-логики являются методы машинного обучения.

Машинное обучение позволяет адаптироваться к новым угрозам за счет непрерывного обучения на исторических и реальных данных: обучение без учителя для выявления неизвестных угроз и аномалий в поведении, обучение с учителем для быстрой идентификации известных типов атак.

Преимущество машинного обучения – динамические профили нормального поведения пользователей и систем. Точность обучения зависит от целостности входных данных. Важно учитывать чувствительность данных.

Глубокое обучение позволяет анализировать сложные структуры данных для обнаружения скрытых зависимостей, недоступных классическим алгоритмам. Важно отметить, что вместо единой модели эффективнее использовать архитектуру, состоящую из нескольких моделей.

Интеллектуальные методы находят применение в ключевых функциях систем мониторинга: от обработки естественного языка, упрощающей взаимодействие с системой через NLP-запросы, до поведенческого анализа, необходимого для предотвращения несанкционированного доступа.

Интеграция ИИ трансформирует SIEM, превращая ее в проактивную платформу защиты со следующими возможностями:

- минимизация ложных срабатываний, фиксация реальных угроз;
- обнаружение ранее неизвестных угроз;
- выявление сложных и распределенных во времени атак;
- предотвращение инцидентов на начальных стадиях (разведки).

Ожидается, что дальнейшее развитие интеллектуальных алгоритмов приведет к появлению систем обнаружения и реагирования, минимизирующих участие человека в решении однотипных задач.

Заключение

Интеграция технологий искусственного интеллекта является ключевым направлением эволюции SIEM, и повышает эффективность обнаружения сложных угроз, улучшает качество корреляции событий, снижает уровень нагрузки на специалистов информационной безопасности, ускоряет процесс реагирования на инциденты.

К сдерживающим факторам можно отнести необходимость качественных и не всегда стандартных данных для обучения, риск ошибок при некорректной настройке параметров, сложность интерпретации конкретных выводов, высокие требования к вычислительным ресурсам.

Наиболее перспективным подходом выглядит гибридная модель, сочетающая логику классических правил корреляции с адаптивными возможностями технологий искусственного интеллекта.

Список использованных источников

1. Рубанова К. В., Голуб А. А. (2025) Сравнительный анализ SIEM для киберцентров. *Сборник материалов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР*. 34–37.
2. Алейникова Д. И. (2025) Системы управления информационной безопасностью и событиями информационной безопасности. *Технические средства защиты информации*. 51–54.
3. Булгакова Е. В., Дойников Д. С., Кубанков А. Н. (2026) Проблема точности и объяснимости при внедрении искусственного интеллекта в системы управления информацией и событиями безопасности. *Наукоемкие технологии в космических исследованиях Земли*. 17 (3) 35–41.

References

1. Rubanova K. V., Golub A. A. (2025) Comparative Analysis of SIEM for Cyber Centers. *Collection of Materials of the 61st Scientific Conference of Postgraduates, Master Students and Students of BSUIR*. 34–37.
2. Aleinikova D. I. (2025) Information Security and Information Security Event Management Systems. *Technical Means of Information Protection*. 51–54.
3. Bulgakova, E. V., Doinikov, D. S., Kubankov, A. N. (2026). The Problem of Accuracy and Explainability in the Implementation of Artificial Intelligence in Security Information and Event Management Systems. *High-Tech Technologies in Earth Space Exploration*. 17 (3) 35–41.

Сведения об авторах

Славинский Г.А., магистрант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», gr.slavin.sci@mail.ru.

Быстрова В.А., магистрант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», veronikabystrova94@gmail.com.

Боброва Н.Л., доцент, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», bobrova@bsuir.by.

Information about the authors

Slavinsky G.A., master's degree student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, gr.slavin.sci@mail.ru.

Bystrova V.A., master's degree student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, veronikabystrova94@gmail.com.

Bobrova N.L., associate professor, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, bobrova@bsuir.by.

UDC 537.874.6

ELECTRODYNAMIC ANALYSIS OF NANOCOMPOSITE MICROWAVE SCREENING VIA EQUIVALENT *RLC* CIRCUIT MODELS

Y. Wu, S.L. Prischepa

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. This study presents an electrodynamic analysis of hybrid nanocomposites consisting of carbon nanotubes (CNTs) with embedded ferromagnetic nanoparticles for microwave screening. By utilizing equivalent parallel and series *RLC* circuit models, we demonstrate that these materials offer a unique combination of broadband shielding and tunable resonance. Experimental parameters for resistance (*R*), capacitance (*C*), and inductance (*L*) were mapped to the physical morphology of the nanocomposite, revealing that the integration of magnetic nanoparticles significantly enhances the inductive response and absorption characteristics. Results indicate that while parallel networks provide stable broadband attenuation, series configurations enable frequency-selective screening, making these hybrids ideal for high-frequency applications in 5G/6G and aerospace sectors.

Keywords: resistance; capacitance; inductance; carbon nanotubes; ferromagnetic nanoparticles; series circuit; fully parallel circuit; impedance; screening efficiency; *RLC* circuit.

Introduction

The rise of high-frequency electronics has turned the electromagnetic (EM) spectrum into a crowded space. To keep electronic “noise” from degrading sensitive devices, nanocomposites are widely used nowadays. Among these, polymer-based nanocomposites reinforced with conductive fillers like carbon nanotubes (CNTs) with embedded Fe nanoparticles [1] have emerged as frontrunners [2]. While full-wave numerical simulations provide high accuracy, equivalent *RLC* circuit modeling offers a computationally efficient alternative, providing deep physical insight into the interaction between microwave radiation and the microscopic morphology of the composite. Moreover, treating a nanocomposite as an equivalent series or parallel *RLC*

(resistor–inductor–capacitor) circuit allows predicting its shielding effectiveness (SE) without detailed quantum-level analysis [3].

In a nanocomposite, the electromagnetic response is governed by three primary phenomena:

1. Ohmic Loss (R): The movement of charge carriers through the conductive filler network.
2. Polarization and Capacitive Storage (C): The accumulation of charge at the interfaces between conductive fillers and the insulating polymer matrix (Maxwell-Wagner-Sillars effect).
3. Self-Inductance (L): The magnetic energy stored due to the current loops and the intrinsic magnetic properties of embedded ferromagnetic nanoparticles.

Model Simulation

We consider two types of RLC circuits: series and parallel. In a series configuration, the components are arranged in a single path. This model is often used to describe nanocomposites in which the conductive fillers are sparse (below the percolation threshold) or in which the material behaves like a thin, capacitive barrier. The total impedance (Z_s) of a series RLC circuit is given by

$$Z_s = R + j\omega L + \frac{1}{j\omega C}, \quad (1)$$

where $\omega = 2\pi f$ is the angular frequency. At the resonance frequency ($f_0 = \frac{1}{2\pi\sqrt{LC}}$), the inductive and capacitive reactances cancel each other out.

At low frequency, the capacitor dominates ($1/j\omega C$ is large), leading to high impedance and high reflection. At resonance, impedance is at its minimum (equal to R). This is often where the material is most "transparent" or where absorption peaks depend on the matching to free space (377 Ohm). Finally, at high frequency, the inductor dominates ($j\omega L$), causing the shielding effectiveness to rise again as the material resists changes in current.

The fully parallel RLC circuit is the preferred model for nanocomposites that have reached the percolation threshold. Then the fillers form continuous conductive networks that allow for "bulk" current flow. The equivalent impedance (Z_p) is then

$$Z_p = \frac{1}{\sqrt{\left(\frac{1}{R}\right)^2 + \left(\omega C - \frac{1}{\omega L}\right)^2}} \quad (2)$$

It follows from Eq. (2) that because the components are in parallel, the branch with the lowest impedance dictates the behavior. If R is very low (high conductivity), the material acts as a highly reflective "Faraday Cage." At the frequency where $\omega C = 1/\omega L$, the impedance Z_p reaches its maximum. This can be strategically tuned to create "band-stop" filters where the material selectively blocks or allows specific microwave frequencies. Finally, it should be noted that

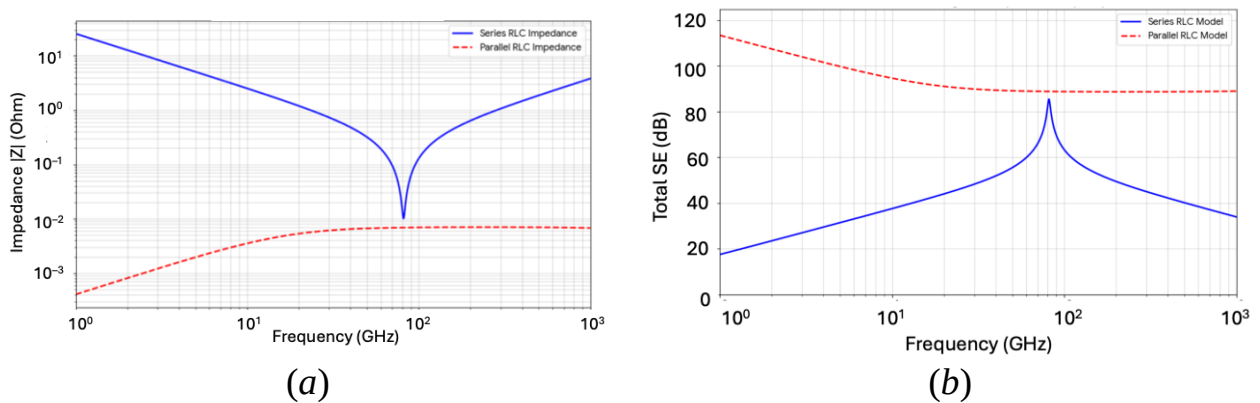
parallel circuits generally provide a more accurate representation of the wideband shielding seen in dense carbon-based composites.

Based on the above considerations and on the approach of the evaluation of the permittivity and permeability of a CNT-based nanocomposite filled with Fe nanoparticles [2,4], it is possible to estimate the screening efficiency (SE), which refers to the ability of the nanocomposite to attenuate EM interference or to shield internal electric fields from external influence. In an RLC network representing a nanocomposite, the screening efficiency is a measure of the ratio between the incident power (P_I) and the transmitted power (P_T), $SE = 10\log_{10}\left(\frac{P_I}{P_T}\right)$. In the RLC framework, this power loss is determined by three physical mechanisms: Reflection (Re), Absorption (A), and Multiple Reflections (M). Then the total screening efficiency is the sum of these three components,

$$SE_{Total} = SE_{Re} + SE_A + SE_M \quad (3)$$

All the components of the Eq. (3) can be calculated considering real parameters of the RLC circuit. In this work, we employ the following characteristic parameters: $R=0.003\text{--}0.015$ (0.002–0.01) Ohm, $C=1\text{--}15$ (1–10) pF, and $L=0.22\text{--}1.8$ (0.01–0.1) pH for series (parallel) circuit, which are typical for CNT-based nanocomposites [3,4].

The results of the calculated impedance and total SE versus frequency for both parallel and series configurations for a fixed parameter values from the above intervals are presented in Figures 1a and 1b, respectively.



a – Magnitude of impedance $|Z|$ versus frequency; (b) – Microwave screening efficiency (SE) versus frequency

The resonance frequency determines the "tuning" of the material – the specific frequency at which the material's inductive and capacitive behaviors balance each other out. It was obtained that, for series RLC circuit, using given ranges of the parameters, the resonance frequency falls within the 29.06 to 251.65 GHz range. This makes the series-mode nanocomposite highly relevant for 5G/6G communication bands and millimeter-wave radar shielding. For

parallel *RLC* model, the resonance shifts significantly higher, spanning 129.95 GHz to 1.59 THz. This, in turn, indicates that the parallel-coupled network is better suited for sub-terahertz and terahertz applications. At the midpoint resonance, the impedance drops to its minimum value (the ohmic resistance). Because Z becomes small (10^{-2} Ohm), the material acts as a near-perfect conductor at this frequency. This results in a sharp spike in *SE*, reaching over 80 dB. Away from resonance, the *SE* drops as the capacitive reactance (at low frequencies) or inductive reactance (at high frequencies) increases the total impedance, allowing more EM energy to pass through.

The parallel configuration represents a well-percolated network where conductive pathways are abundant. Unlike the series model, the parallel circuit maintains an extremely low impedance (between 10^{-4} and 10^{-2} Ohm) across almost the entire microwave and millimeter-wave spectrum. Because the total impedance remains consistently much lower than the impedance of free space, the *SE* is exceptionally high and stable, maintaining values above 90 dB. The "anti-resonance" (where impedance would peak) occurs much higher in the THz range, meaning that for standard microwave applications, this material acts as a consistent, high-performance shield.

Conclusion

The synergy between CNT and high-permeability Fe nanoparticles creates a material that transcends the limitations of single-component shields. While CNTs provide the baseline conductivity for reflection, the magnetic inclusions enable tunable absorption and superior impedance matching. By adjusting the *RLC* parameters – specifically the inductance through nanoparticle loading and capacitance through polymer spacing – it is possible to design "smart" shields. These nanocomposites are uniquely positioned to meet the rigorous demands of next-generation telecommunications and aerospace applications, where lightweight, broadband, and tunable EMI protection is paramount.

The obtained results demonstrate that, if CNT-based nanocomposite is synthesized such that fillers act in series (e.g., layered or aligned structures), it can be used as a frequency-selective surface. It will provide maximum protection at a specific band while being relatively more transparent at lower frequencies. If, vice versa, the material is synthesized to form a dense, isotropic 3D network (above the percolation threshold), it will serve as a superior broadband shield. It is ideal for military or high-precision laboratory environments where total suppression of signals from 1 GHz to 1 THz is required.

References

1. Danilyuk A.L., Komissarov I.V., Labunov V.A., Le Normand F., Derory A., Hernandez J.M., et al. (2015) Manifestation of Coherent Magnetic Anisotropy in a Carbon Nanotube Matrix with Low Ferromagnetic Nanoparticle Content. *New Journal of Physics*. 17(2), 023073.
2. Gupta S., Tai N. (2019) Carbon Materials and their Composites for Electromagnetic Interference Shielding Effectiveness in X-band. *Carbon*. 152, 159–187.
3. Atdayev A., Danilyuk A. L., Prischepa S. L. (2015) Interaction of Electromagnetic Radiation in the 20–200 GHz Frequency Range with Arrays of Carbon Nanotubes with Ferromagnetic Nanoparticles. *Beilstein Journal of Nanotechnology*. 6, 1056–1064.
4. Labunov V. A., Danilyuk A. L., Prudnikava A. L., Komissarov I., Shulitski B. G., Speisser C., et al. (2012) Microwave Absorption in Nanocomposite Material of Magnetically Functionalized Carbon Nanotubes. *Journal of Applied Physics*. 112 (2), 024302.

Information about the authors

Wu Y., master student, Department of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, ilmsiaoms@gmail.com.

Prischepa S.L., Dr. of Sci. (Phys. and Math.), Professor, Professor at the Department of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, prischepa@bsuir.by.

УДК 546.303

КОНВЕРСИЯ СПИНОВОГО ТОКА В ЗАРЯДОВЫЙ В МАГНИТНОМ ПОЛУМЕТАЛЛЕ ВЕЙЛЯ

А.С. Силивонец, А.Л. Данилюк

Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной работе с помощью модели на основе полуклассического уравнения Больцмана получены результаты моделирования конверсии спинового тока в зарядовый в гетероструктуре, состоящей из ферромагнитного металла и одно-, дву- и трехмерного полуметалла Вейля, для баллистического и диффузионного режимов переноса заряда. Установлено, что эффективность преобразования спина в зарядовый ток в целом снижается с ростом отношения длины полуметалла Вейля к длине свободного пробега электронов в нем.

Ключевые слова: спиновый ток, конверсия, полуметалл Вейля, проводимость.

CONVERSION OF SPIN CURRENT TO CHARGE CURRENT IN A MAGNETIC WEYL SEMIMETAL

A.S. Silivonets, A.L. Danilyuk

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. In this paper, using a model based on the semiclassical Boltzmann equation, the results of modeling the conversion of a spin current into a charge current in a heterostructure

consisting of a ferromagnetic metal and a one-, two-, and three-dimensional Weyl semi-metal for ballistic and diffusion charge transfer modes are obtained. It has been established that the efficiency of the spin-to-charge current conversion generally decreases with an increase in the ratio of the length of the Weyl semimetal to the mean free path of the electrons in it.

Keywords: spin current, conversion, Weyl semimetal, conductivity.

Введение

В данной работе получены результаты моделирования значений токов в одно- (1D), дву- (2D) и трехмерной (3D) модели магнитного полуметалла Вейля (MWSM) [3]. Для нормировки расчетов вводится параметр $\alpha = L_x/l_f$, где L_x – длина проводника, l_f – длина свободного пробега электрона.

Основная часть

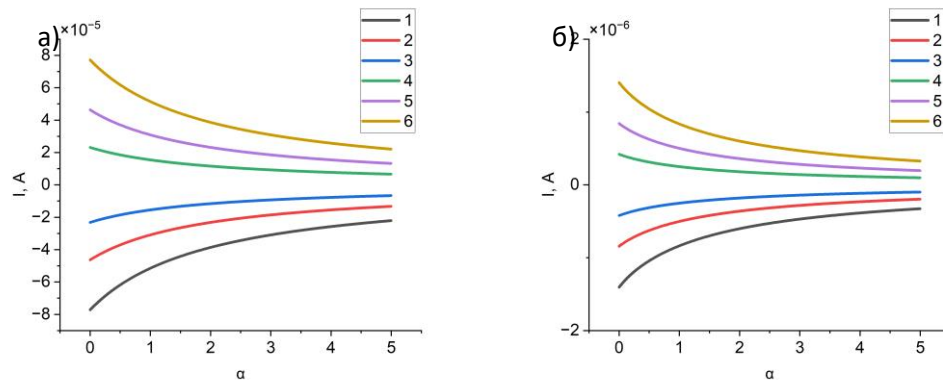
Одномерный случай. Поскольку электрический ток I постоянен вдоль направления x , его величина вычисляется, задавая $x = L_x/2$, что дает следующее выражение [2]

$$I = \frac{2e}{h} \int v_x g(k_x, x = \frac{L_x}{2}) \left(-\frac{\partial f_0}{\partial \varepsilon_k} \right) dk_x = G^{1D} (V_L - V_R), \quad (1)$$

$$\text{где } G^{1D} = G_0^{1D} \frac{2l_f}{L_x + 2l_f}, \quad (2)$$

это проводимость системы.

Полученные зависимости значения тока при изменении значения α для падения потенциала на MWSM $\Delta V = V_L - V_R \{-1; -0,6; -0,3; 0,3; 0,6; 1\}$ В показаны на рисунке а).



а) – Зависимости значений тока I от α при различных $\Delta V = V_L - V_R$: $\Delta V = -1$ В (кривая 1), $-0,6$ В (кривая 2), $-0,3$ В (кривая 3), $0,3$ В (кривая 4), $0,6$ В (кривая 5), $1,0$ В (кривая 6).

Рисунок 1б) – Зависимость значения тока I от α при $\Delta V = \{-1; -0,6; -0,3; 0,3; 0,6; 1\}$ В

Двумерный случай. Значение тока для двумерного случая будет определяться по формуле

$$I = G^{2D} (V_L - V_R),$$

где [2]

$$G^{2D} = G_0^{2D}(\chi_{bal}^{2D} + \chi_{dif}^{2D}) \quad (3)$$

это проводимость двумерного образца, где χ_{bal}^{2D} и χ_{dif}^{2D} – баллистический и диффузионный вклад в проводимость.

Зависимость значения тока будет выявляться при изменении значения α при $\Delta V = \{-1; -0,6; -0,3; 0,3; 0,6; 1\}$ В, что показано на рисунке 1б).

Трехмерный случай. В трехмерном случае проводимость равна

$$G^{3D} = G_0^{3D}(\chi_{bal}^{3D} + \chi_{dif}^{3D}) \quad (4)$$

где $G_0^{3D} = N_{ch} e^2 / h$ с $N_{ch} = (2\pi k_F^2 / h^2) A$ с A в качестве поперечного сечения.

Заключение

Путем моделирования на основе полуклассического уравнения Больцмана установлены закономерности конверсии спинового тока в зарядовый в гетероструктуре ферромагнетик/магнитный полуметалл Вейля. Рассмотрены одно-, дву- и трехмерный случаи полуметалла Вейля в баллистическом и диффузионном режимах токопереноса. Установлено, что эффективность преобразования спин/заряд снижается с ростом отношения длины магнитного полуметалла Вейля к длине свободного пробега электронов в нем. Установленные закономерности конверсии спинового тока в зарядовый важны для разработки энергоэффективных спинтронных устройств.

Список использованных источников

1. Zhang S.S.-L., et al. (2019) Spin-to-Charge Conversion in Magnetic Weyl Semimetals. *Phys. Rev. Lett.* 123 (18), 187201..
2. Ge Y.F., et al. (2022) The effect of size on spin-to-charge conversion in the magnetic Weyl semimetal. *Physics Letters A.* 429, 127953.
3. Geng H., et al. (2016) Unified semiclassical approach to electronic transport from diffusive to ballistic regimes. *Chin. Phys. B.* 25 (9), 097201.

References

1. Zhang S.S.-L., et al. (2019) Spin-to-Charge Conversion in Magnetic Weyl Semimetals. *Phys. Rev. Lett.* 123 (18), 187201..
2. Ge Y.F., et al. (2022) The effect of size on spin-to-charge conversion in the magnetic Weyl semimetal. *Physics Letters A.* 429, 127953.
3. Geng H., et al. (2016) Unified semiclassical approach to electronic transport from diffusive to ballistic regimes. *Chin. Phys. B.* 25 (9), 097201.

Сведения об авторах

Силивонец А.С., магистрант кафедры микро- и нанoeлектроники, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники, adefols12@gmail.com

Данилюк А.Л., к.ф.-м.н., доцент, доцент кафедры микро- и нанoeлектроники, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники, danilyuk@bsuir.by.

Information about the authors

Silivonets A.S. undergraduate at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Danilyuk A.L., Cand. of Sci., Associate Professor, Associate Professor at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

УДК 004.8-049.5

АРХИТЕКТУРА МОДУЛЯ ИИ-АГЕНТА ДЛЯ SIEM-СИСТЕМ НОВОГО ПОКОЛЕНИЯ

Е.И. Юнчиц, П.Б. Гусаков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается проблема перегрузки операторов безопасности ложными срабатываниями в традиционных системах SIEM. Предложена архитектура автономного ИИ-агента, внедряемого в средство защиты как функциональный элемент. Агент использует методы машинного обучения для анализа событий и автоматического реагирования на инциденты. Результаты моделирования показывают снижение нагрузки на аналитиков до 40%.

Ключевые слова: Искусственный интеллект; SIEM; машинное обучение; SOC; информационная безопасность; логи; инциденты; SOAR; аналитика; SHAP.

AI-AGENT MODULE ARCHITECTURE FOR NEXT-GENERATION SIEM SYSTEMS

E.I. Yunchits, P.B. Gusakov

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. This article examines the problem of security operator overload with false positives in traditional SIEM systems. We propose the architecture of an autonomous AI agent, which can be embedded into the security solution as a functional element. The agent uses machine learning methods to analyze events and automatically respond to incidents. Simulation results show a reduction in analyst workload of up to 40%.

Keywords: Artificial intelligence; SIEM; machine learning; SOC; information security; logs; incidents; SOAR; analytics; SHAP.

Введение

SIEM-системы – центральный компонент мониторинга ИТ-инфраструктур. Рост объема логов и сложности атак увеличивает количество ложных срабатываний, отвлекающих SOC на неопасные инциденты. Это снижает эффективность и повышает риск пропуска реальных угроз. Внедрение ИИ-агентов позволит моментально реагировать на события кибербезопасности и заранее выявлять подозрительные действия злоумышленников.

Основная часть

ИИ-агент – программный модуль с понятными интерфейсами, встраиваемый в инфраструктуру. Архитектура включает три уровня: сбор данных, анализ угроз и ответные действия, повторяя схему современных SIEM (прием событий, аналитика, реагирование). Это обеспечивает легкую интеграцию.

На первом уровне выполняется нормализация логов по стандарту CIM (Common Information Model). Разнородные сообщения приводятся к единому формату. Без обработки алгоритмы работают нестабильно, а именно: события теряются, картина искажается. Качество данных определяет до 80% успеха внедрения ИИ[1].

Второй уровень представляет собой само ядро ИИ-агента. Здесь используются модели машинного обучения без учителя. Модели запоминают поведение пользователей и различных систем, фиксируют паттерны этого поведения и сообщают об отклонениях, снижая этим количество ложных срабатываний. Также увеличивается скорость обнаружения сложных атак [2].

Третий уровень обеспечивает взаимодействие с SOAR [3] и автоматизированные действия. При срабатывании агент изолирует хост, блокирует учетную запись и уведомляет смену без ручных команд. Сотрудники получают готовые инциденты, что разгружает команду для работы со нестандартными ситуациями.

Для оценки эффективности выполнено сравнение с существующими продуктами[4]. В таблице 1 приведены различия между SIEM-системами без ИИ-агента и SIEM-системами с ИИ-агентом.

Сравнительный анализ традиционных SIEM и систем с ИИ-агентом
на основе реальных продуктов
Comparative analysis of traditional SIEM and AI-agent-based systems using real products

Критерий	SIEM-системы без ИИ-агента	SIEM-системы с ИИ-агентом
Примеры продуктов	IBM QRadar, ArcSight, LogRhythm	Microsoft Sentinel + AI agents, Exabeam Fusion, Splunk ES + ML Toolkit
Уровень ложных срабатываний	60–90% от общего числа алертов	Снижение на 60–80% благодаря поведенческому анализу
Среднее время обнаружения атак	2–6 часов (ручная корреляция)	5–20 минут (автоматическая приоритизация)
Взаимодействие с SOAR	Требует отдельной настройки	Нативная интеграция

Как видно из таблицы выше, добавление ИИ-агентов в современные SIEM (Microsoft Sentinel, Exabeam Fusion, Splunk ES) сильно влияет на основные показатели их работы. По данным из отчетов о внедрении ИИ-агента, можно увидеть, что удастся снизить количество ложных срабатываний примерно на 60-90%. Это позволяет уменьшить нагрузку на аналитиков и дает им больше времени на рассмотрение действительно критичных инцидентов. Также, одновременно с этим сокращается среднее время обнаружения угроз.

Заключение

Ключевая проблема – прозрачность моделей («черный ящик»). Система принимает решение, но не объясняет почему. Для решения в ИИ-агента внедряется компонент интерпретации на основе SHAP, формирующий пояснение о влияющих особенностях поведения.

Вопрос защищенности самого ИИ-агента также важен. Агент должен работать в изолированной среде, иметь ограниченные права и не получать прямого доступа к критичным системам. Обмен данными с SIEM должен проходить через защищенные API-интерфейсы.

Список использованных источников

1. Чувакин А. А., Шмидт К., Филлипс К. Логирование и управление журналами: авторитетное руководство по пониманию концепций логирования и управления журналами. Уолтем: Syngress, 2012. 480 с.

2. Алескер Э. В. (ред.) Технологии машинного обучения в кибербезопасности: учебное пособие. М.: Интернет-университет информационных технологий, 2023. 280 с.
3. Дэрил К., Граймс Дж. Оркестрация безопасности, автоматизация и реагирование для аналитиков безопасности. Бирмингем: Packt Publishing, 2023. 356 с.
4. Европейские платформы SIEM 2026: независимый сравнительный отчет. Текрон, 2026.

References

1. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Waltham: Syngress, 2012. 480 pages.
2. Alesker E. V. (ed.) Machine Learning Technologies in Cybersecurity: Textbook. Moscow: Internet University of Information Technologies, 2023. 280 pages.
3. Daryl K., Grimes J. Security Orchestration, Automation, and Response for Security Analysts. Birmingham: Packt Publishing, 2023. 356 pages.
4. European SIEM Platforms 2026: Independent Comparison Report. Tekron, 2026

Сведения об авторах

Юнчиц Е.И., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», egorynchic2007@gmail.com.

Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», p.gusakov@bsuir.by.

Information about the authors

Yunchits E.I., cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, egorynchic2007@gmail.com.

Gusakov P.B., Master, Head of the Cycle, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, p.gusakov@bsuir.by.

УДК 004.8:004.056.54

ПРИМЕНЕНИЕ ИИ-АГЕНТОВ В ДОВЕРЕННОЙ ЭЛЕМЕНТНОЙ БАЗЕ ДЛЯ ПРЕДИКТИВНОГО ОБНАРУЖЕНИЯ АППАРАТНЫХ АТАК

А.О. Пилипенко, Ф.Н. Супрун

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной статье рассматривается вопрос о защите элементной базы с помощью встроенных ИИ-агентов. В работе анализируется, как ИИ могут находить аппаратные закладки и предотвращать атаки по внешним каналам. Данный подход позволяет сделать защиту элементной базы автоматической и более эффективно.

Ключевые слова: элементная база, защита информации, искусственный интеллект, ИИ-агент, аппаратные средства защиты, кибербезопасность, аппаратный троян, мониторинг сигналов, микросхемы, информационная безопасность.

APPLICATION OF AI AGENTS IN A TRUSTED HARDWARE COMPONENTS FOR PREDICTIVE DETECTION OF HARDWARE ATTACKS.

A.O. Pilipenka, F.N. Suprun

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article examines the protection of hardware components using embedded AI agents. It analyzes how AI can detect hardware bugs and prevent attacks through external channels. This approach makes hardware protection more automated and effective.

Keywords: element base, information protection, artificial intelligence, AI agent, hardware protection, cybersecurity, hardware Trojan, signal monitoring, microcircuits, information security.

Введение

Сегодня элементная база является защитой любой информационной системы, но она чаще всего используется аппаратными атаками. Обычные методы защиты, работающие по заранее прописанным правилам, не всегда могут привести к скрытым угрозам внутри системы. Решением этой проблемы может стать внедрение технологий искусственного интеллекта прямо в аппаратную часть устройства. В данной работе исследуется, как именно такие интеллектуальные компоненты помогают защитить элементные базы и повысить надежность цифровых систем.

Основная часть

Сегодня практически каждое электронное устройство, начиная от обычного смартфона и заканчивая промышленными контроллерами, работает на базе микросхем, которые мы называем элементной базой. Все время считалось, что если программное обеспечение защищено антивирусом или шифрованием, то системе никакая опасность не угрожает. Однако сейчас все чаще говорят об аппаратных атаках, когда злоумышленники пытаются взломать само «железо».

Одной из самых опасных угроз являются аппаратные трояны. Это небольшие изменения в логике работы чипа, которые могут произойти еще во время производства. Такой троян может годами «спать», а затем активироваться по специальному сигналу злоумышленника и передать секретный ключ шифрования хакеру. Главное, как раз то, что найти такую закладку обычными методами практически невозможно из-за большой сложности как раз самих микросхем [1]. Защита «железа» заметно эволюционировала: все началось с обычных проверок данных, таких как контрольные суммы, а по итогу все пришло к созданию чипов TPM. Эти чипы сегодня – отличная база для безопасности компьютера.

В наше время на помощь приходит искусственный интеллект. Если мы встроим небольшой ИИ-агент прямо в сам чип, он сможет работать как внутренний «цифровой охранник». То есть вместо того, чтобы работать по строгим правилам, ИИ-агент самообучается и действует по ситуации. В такой элементной базе выделяют три принципах: предиктивности (предсказании атак), автономности (самостоятельное принятие решений на основе конкретной ситуации) и верифицируемости (подтверждении надежности ИИ-агента).

ИИ-агент работает так: он запоминает, как ведет себя «здоровый» процессор. Например, сколько он потребляет энергии, какова скорость передачи данных и как часто процессор взаимодействует с памятью. Если параметры начинают отклоняться от нормы, например, если энергопотребление резко меняется в момент простоя, то ИИ-агент понимает, что происходит что-то подозрительное [2]. Технически это реализуется через систему сенсоров, собирающих телеметрию (температуру кристалла, тактовую частоту), и моделей ИИ, которые выделяют закономерности атаки среди обычного шума.

Еще один важный момент – это атаки по сторонним каналам (side-channel analysis) [3]. Хакеры научились «слушать» микросхемы, анализируя их электромагнитное излучение или шум в цепях питания. Таким образом можно буквально узнать, какой пароль или ключ обрабатывает чип в данный момент. Обычный контроллер этого не замечает, но интеллектуальный агент постоянно анализирует сигналы «аппаратных логов», поэтому может зафиксировать такого рода кражу информации.

Сложность как раз во внедрении ИИ-агента. Конечно, полноценную нейросеть в маленький чип интегрировать сложно, так как ресурсов (память и питание) просто не хватает. Поэтому в работе используются «легкие» алгоритмы машинного обучения, которые сильно не нагружают устройства. Перспективным направлением здесь является нейроморфная защита на базе спайковых нейронных сетей (Spiking Neural Networks), которые имитируют строение и работу мозга, а также позволяют работать быстро при крайне низком энергопотреблении.

Однако развитие таких систем сталкивается с новыми проблемами, такими как состязательное машинное обучение (Adversarial ML). Злоумышленники могут пытаться «обмануть» ИИ-агента. Хакеры начинают подсовывать ему искаженные данные сенсоров, чтобы скрыть наличие каких-либо неполадок.

На сегодняшний день концепция интеллектуальной защиты на аппаратном уровне уже активно внедряется лидерами ИТ-индустрии. Одним из наиболее известных примеров является технология Intel Threat Detection Technology (Intel TDT). В процессорах Intel Core (начиная с 10-го

поколения) используются блоки телеметрии, которые передают данные о работе процессора в модели машинного обучения. Это позволяет обнаруживать программы-вымогатели (ransomware) и скрытый майнинг криптовалют на уровне микроархитектуры, до того, как их заметит антивирус. В промышленном секторе такие компании, как NVIDIA (блок BlueField DPU) и NXP Semiconductors, разрабатывают специализированные блоки аппаратного ускорения ИИ, которые встроены в сетевые контроллеры.

Заключение

В ходе работы было доказано, что внедрение ИИ-агентов в элементную базу – это отличный способ защиты от скрытых аппаратных угроз. Благодаря постоянному анализу физических параметров, таких как энергопотребление и тайминги, ИИ способны находить аппаратные закладки, которые незаметны на первый взгляд и могут быть недоступны для заранее прописанного программного обеспечения. Разработка такого подхода к защите становится важным этапом в обеспечении безопасности электроники.

Список использованных источников

1. Грибунин В. Г., Васильев С. А. Цифровая стеганография и защита элементной базы. – СПб.: Солон-Пресс, 2021. – 256 с.
2. Безродный Б. Ф. Интеллектуальные системы защиты информации в микроэлектронике // Вестник кибербезопасности. – 2023. – № 2. – С. 15-22.
3. Куприянов М. С. Проектирование защищенных микропроцессорных систем. – СПб.: БХВ-Петербург, 2020. – 320 с.

References

1. Gribunin V. G., Vasiliev S. A. Digital Steganography and Protection of the Element Base. St. Petersburg: Solon-Press, 2021. 256 p.
2. Bezrodny B. F. Intelligent Information Security Systems in Microelectronics // Cybersecurity Bulletin. 2023. No. 2. pp. 15-22.
3. Kupriyanov M. S. Design of Secure Microprocessor Systems. St. Petersburg: BHV-Petersburg, 2020. 320 p.

Сведения об авторах

Пилипенко А.О., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pilipenkoandrej602@gmail.com.

Супрун Ф.Н., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», f.suprun@gmail.com

Information about the authors

Pilipenko A. O., cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, pilipenkoandrej602@gmail.com.

Suprun, teacher, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, f.suprun@gmail.com

УДК 004.272, 004.31

РЕАЛИЗАЦИЯ НА FPGA АЛГОРИТМА ШИФРОВАНИЯ СТБ 34.101.31

М.В. Качинский, А.В.Станкевич, А.И.Шемаров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается реализация алгоритма шифрования блока СТБ 34.101.31 на базе программируемой логической интегральной схемы (ПЛИС) с архитектурой field-programmable gate array (FPGA), обладающая более высокой производительностью по сравнению с известными. Описываются архитектурные особенности реализации. Приводится сравнение аппаратных затрат и производительности предлагаемой реализации с известными решениями.

Ключевые слова: СТБ 34.101.31; алгоритм шифрования блока; реализация на FPGA; итерация; блок данных; ключ; раунд алгоритма; итеративная, конвейерная архитектура процессора; аппаратные ресурсы кристалла FPGA; производительность.

FPGA IMPLEMENTATION OF THE STB 34.101.31 ENCRYPTION ALGORITHM

M.V. Kachinsky, A.V. Stankevich, A.I. Shemarov

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. This article discusses an implementation of the STB 34.101.31 encryption algorithm based on a field-programmable gate array (FPGA) architecture, which offers higher performance than existing solutions. The architectural features of the implementation are described. A comparison of the hardware costs and performance of the proposed implementation with existing solutions is provided.

Keywords: STB 34.101.31; block encryption algorithm; FPGA implementation; iteration; data block; key; algorithm round; iterative, pipelined processor architecture; FPGA hardware resources; performance.

Введение

Алгоритм шифрования блока является базовым алгоритмом СТБ 34.101.31 для различных режимов шифрования, выработки имитовставки и других алгоритмов стандарта. Производительность его реализации будет существенно определять общую производительность реализаций

упомянутых алгоритмов. При необходимости высокопроизводительной реализации алгоритмов стандарта требуется их аппаратная реализация.

Основная часть

СТБ 34.101.31 описывает блочный алгоритм шифрования с размером блока 128 бит и длиной ключа 256 бит. Алгоритм шифрования блока выполняется за 8 раундов, каждый раунд имеет 9 вычислительных шагов.

В результате анализа известных источников были найдены две статьи [1, 2], описывающие реализации на FPGA алгоритма режима простой замены СТБ 34.101.31. В этом режиме исходное сообщение разбивается на блоки по 128 бит, которые поблочно шифруются алгоритмом шифрования блока.

Режим простой замены на практике используется редко из-за повторения зашифрованных значений для одинаковых блоков данных. Для режимов сцепления блоков и гаммирования с обратной связью использование конвейерной архитектуры не эффективно с точки зрения аппаратных затрат в связи с тем, что для шифрования следующего блока необходимо дожидаться завершения шифрования предыдущего блока. Поэтому для последующего сравнительного анализа конвейерные реализации [2] рассматривать не будем и выберем наиболее производительную реализацию Belt_par из статьи [1] и последовательную реализацию из статьи [2].

Одним из преобразований алгоритма СТБ 34.101.31 является подстановка, задаваемая таблицей из 256 8-разрядных значений. Для реализации таблицы подстановки проект Belt_par использует блочную память FPGA (RAMB16s), последовательная реализация [2] для этой цели использует распределенную память кристалла FPGA.

Предлагаемая реализация имеет следующие особенности:

Блок памяти (RAMB16 или RAMB18E в зависимости от ПЛИС) сконфигурирован как двухпортовый, что позволяет одновременно и независимо обращаться к каждой ячейке памяти по двум портам. В одном блоке памяти хранится одна таблица подстановки H . За счет независимой адресации к этой таблице по портам A и B с помощью одного блока реализуется две подстановки $H(u_i)$;

Предлагаемая реализация предусматривает максимально возможное распараллеливание шагов алгоритма. Один раунд алгоритма выполняется за 5 тактов. При этом одновременно не будет использоваться более двух преобразований Gr , каждое из которых требует применения 4 таблиц подстановки. Общее число блоков памяти для двух преобразований Gr – 4.

Для доступа к таблицам подстановки на разных шагах алгоритма используются мультиплексоры;

Для уменьшения числа использованных LUT в предлагаемой реализации широко используются трехвходовые сумматоры.

Реализации [1, 2] выполнены на устаревших кристаллах FPGA, которые современная среда проектирования Vivado уже не поддерживает. С целью получения результатов для сравнения были выполнены следующие три варианта предлагаемой реализации (характеристики реализаций после процедур размещения и трассировки кристалла ПЛИС приведены в таблице):

Реализация 1 на базе ПЛИС xc3s400-5-fg456 с использованием среды проектирования ISE 14.7 для сравнения с реализацией Belt_par [1];

Реализация 2 на базе ПЛИС xc6vlx130t-1-ff1156 с использованием среды проектирования ISE 14.7 для сравнения с последовательной реализацией [2];

Реализация 3 на базе современной ПЛИС xsku3p-ffvb676-2-e с использованием среды проектирования Vivado.

Приведенные результаты свидетельствуют о более высокой производительности предложенной реализации по сравнению с известными при относительно небольших аппаратных затратах и реализации как зашифрования, так и расшифрования блока.

Характеристики реализаций алгоритма шифрования блока СТБ 34.101.31
Characteristics of implementations of the STB 34.101.31 block encryption algorithm

Характеристика	Предлагаемая реализация			Belt_par [1]	Последовательная [2]
	1	2	3		
Slice Flip Flops	747	776	748	302	847
LUTs	2065	1357	1304	2050	1173
RAMB	4	4	4	28	-
Количество тактов на один блок данных	43	43	43	211	66
Тактовая частота, МГц	66	133	290	–	112
Производительность, Мбит/с	196	395	863	–	217

Заключение

Предложена реализация алгоритма шифрования блока СТБ 34.101.31 на базе FPGA, обладающая более высокой производительностью по сравнению с известными реализациями при относительно небольших аппаратных затратах. Реализация может быть использована для любых режимов шифрования стандарта.

Список использованных источников

1. Поляков А.С., Самсонов В.Е. (2011) Характеристики аппаратной реализации некоторых симметричных алгоритмов шифрования. *Информатика*. (1), 89-94.
2. Ланкевич Ю. Ю. (2013) Процессор алгоритма шифрования «Belt» на базе ПЛИС. *Материалы международной научной конференции «Информационные технологии и системы 2013»* (ИТС 2013). 190–191.

References

1. Poljakov .A.S., Samsonov V.E. (2011) Hardware implementation performances of some symmetric encryption algorithms. *Informatics*. (1), 89-94.
2. Lankevich Y.Y. (2013) FPGA-based Belt encryption algorithm processor. *Information Technologies and Systems 2013 (ITS 2013). Proceeding of The International Conference*. 190–191.

Сведения об авторах

Качинский М.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kachinsky@bsuir.by.

Станкевич А.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stankevich@bsuir.by.

Шемаров А.И., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», shemarov@bsuir.by.

Information about the authors

Kachinsky M., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, kachinsky@bsuir.by

Stankevich A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, stankevich@bsuir.by.

Shemarov A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, shemarov@bsuir.by

УДК 004.272, 004.31

РАСПАРАЛЛЕЛИВАНИЕ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ ДАННЫХ СО СЦЕПЛЕНИЕМ БЛОКОВ

М. В. Качинский, А. В. Станкевич, А. И. Шемаров

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Блочные алгоритмы шифрования находят широкое применение для решения задач в области практической криптографии. Ряд модификаций алгоритмов блочного шифрования, например, при реализации алгоритмов со сцеплением блоков, требуют значительного времени шифрования большого потока данных за счет последовательной обработки блоков. Предлагается режим распараллеливания алгоритма блочного шифрования данных со сцеплением блоков путем линейной декомпозиции входного потока данных.

Ключевые слова: Шифрование, алгоритм блочного шифрования, сцепление блоков, блок, ключ, синхропосылка, декомпозиция потока данных, распараллеливание, программируемое логическое устройство.

PARALLELIZATION OF A BLOCK CIPHER ALGORITHM WITH CIPHER BLOCK CHAINING

M.V. Kachinsky, A.V. Stankevich, A.I. Shemarov

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. Block encryption algorithms are widely used to solve problems in practical cryptography. Some modifications of block encryption algorithms, such as those cipher block chaining algorithms, require significant time to encrypt a large data stream due to sequential processing of blocks. A mode for parallelizing a block encryption algorithm with block chaining through linear decomposition of the input data stream is proposed.

Keywords: Encryption, block cipher algorithm, block chaining, block, key, initialization vector, data flow decomposition, parallelization, programmable logic device.

Введение

Блочные алгоритмы шифрования находят широкое применение для решения задач в области практической криптографии. Оборудование, использующее блочные алгоритмы для шифрования данных с симметричным ключом, появилось достаточно давно. Применение специализированных вычислительных аппаратных средств позволило увеличить эффективность систем безопасности. Эволюция аппаратных комплексов шифрования определялась в первую очередь элементной базой. Коренным образом подход к решению задач шифрования изменился в связи с появлением программируемых логических устройств.

С повышением количества элементов в программируемой логической микросхеме появляется возможность использования все более и более сложных алгоритмов. Алгоритмы блочного шифрования обычно хорошо распараллеливаются и конвейеризируются, что позволяет легко масштабировать аппаратные решения, но только для тех модификаций алгоритма, которые не используют предыдущий зашифрованный блок для обработки следующего блока.

Основная часть

Прогресс в области создания и совершенствования оборудования в итоге приводит к увеличению размеров обрабатываемых потоков данных. Ряд модификаций алгоритмов блочного шифрования, позволяющих получать хорошую криптостойкость, например, при реализации алгоритмов со сцеплением блоков, требуют значительного времени шифрования большого потока данных за счет последовательной обработки блоков. Это связано не с тем, что не существует теоретической возможности распараллеливания процесса шифрования в этих режимах, а определяется жесткой регламентацией процессов шифрования, регулируемых действующими стандартами. Стандарты, в итоге модифицируются и изменяются в соответствии с новыми требованиями, предъявляемыми развитием информационной инфраструктуры и задачами, решаемыми на конкретном этапе создания и развития информационных систем, но этот процесс достаточно медленный.

В работе предлагается режим распараллеливания алгоритма блочного шифрования со сцеплением блоков. Идея способа заключается в возможности декомпозиции шифруемого потока на отдельные потоки. В стандартах блочного шифрования не накладываются жесткие ограничения на количество потоков данных, которые могут быть зашифрованы с помощью одного ключа. Поэтому шифрование разделенных потоков может осуществляться параллельными структурами. Количество одновременно обрабатываемых потоков определяется только существующей в конкретный момент времени технологией создания микросхем требуемой степени интеграции. Однако для реализации алгоритмов блочного шифрования со сцеплением блоков требуется задание начального вектора или синхропосылки. На количество используемых одновременно синхропосылок обычно накладываются ограничения, так как это может теоретически приводить к дискредитации ключа при определенном наборе данных.

Для того чтобы не использовать несколько различных синхропосылок, что затрудняет реализацию алгоритма, или одну и ту же

синхропосылку для шифрования различных потоков, что может снизить криптостойкость алгоритма в целом, предлагается следующий режим работы. Шифрование потока начинается как одного целого потока данных, а далее, после шифрования требуемого количества блоков, определяемого количеством подпотоков, на которые будет разделен исходный поток (определяется количеством параллельно работающих устройств шифрования), происходит декомпозиция потоков. Процесс шифрования в этот случае распараллеливается. Иллюстрация режима распараллеливания потока данных на восемь потоков при реализации алгоритма блочного шифрования со сцеплением блоков приведена в таблице «Распараллеливание потока данных для шифрования».

Заключение

Таким образом, путем декомпозиции входного потока данных, может быть достигнута возможность введения режима распараллеливания алгоритма блочного шифрования данных со сцеплением блоков. В работе приведен линейный алгоритм распределения блоков между устройствами шифрования. Для повышения криптостойкости можно использовать нелинейное распределение блоков по устройствам шифрования.

Распараллеливание потока данных для шифрования
Data flow parallelization for encryption

№ Итерации	УШ 0	УШ 1	УШ 2	УШ 3	УШ 4	УШ 5	УШ 6	УШ 7
0	Синхро-посылка							
1	Блок0							
2	Блок1							
3	Блок2							
4	Блок3							
5	Блок4							
6	Блок5							
7	Блок6							
8	Блок7							
9	Блок15	Блок14	Блок13	Блок12	Блок11	Блок10	Блок9	Блок8
10	Блок23	Блок22	Блок21	Блок20	Блок19	Блок18	Блок17	Блок16
11	...	...	...	...	...	...	...	...

УШ – Устройство шифрования

Сведения об авторах

Качинский М.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kachinsky@bsuir.by.

Станкевич А.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stankevich@bsuir.by.

Шемаров А.И., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», shemarov@bsuir.by.

Information about the authors

Kachinsky M., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kachinsky@bsuir.by

Stankevich A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", stankevich@bsuir.by.

Shemarov A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", shemarov@bsuir.by

УДК 004.056

АРХИТЕКТУРА ПЛАТФОРМЫ АВТОМАТИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.А. Биюмен, К.Ц. Маршалова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье представлена архитектура платформы для автоматизации аудитов информационной безопасности. Описан подход, объединяющий пассивный сбор данных, копирование веб-ресурсов и фильтрацию машинного трафика. Предложен эвристический алгоритм извлечения персональных данных на основе контекстной близости элементов веб-страниц. Использование микросервисной архитектуры и изолированной маршрутизации обеспечивает объективность оценки устойчивости персонала к целевым атакам методами социальной инженерии.

Ключевые слова: информационная безопасность; социальная инженерия; программная архитектура; пассивный сбор данных; эвристический алгоритм; копирование ресурсов; маршрутизация трафика; фильтрация событий; имитация атак; оценка уязвимостей.

SOFTWARE COMPLEX ARCHITECTURE FOR AUTOMATED INFORMATION SECURITY AUDITS

Y.A. Biyumen, K.C. Marshalava

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article presents a platform architecture for automating information security audits. It describes an approach combining passive data collection, resource copying, and machine traffic filtering. A heuristic algorithm for extracting personal data based on contextual proximity is proposed. Microservice architecture and isolated routing ensure objective assessment of personnel resilience to social engineering attacks.

Keywords: Information security; social engineering; software architecture; passive data collection; heuristic algorithm; resource copying; traffic routing; event filtering; attack simulation; vulnerability assessment.

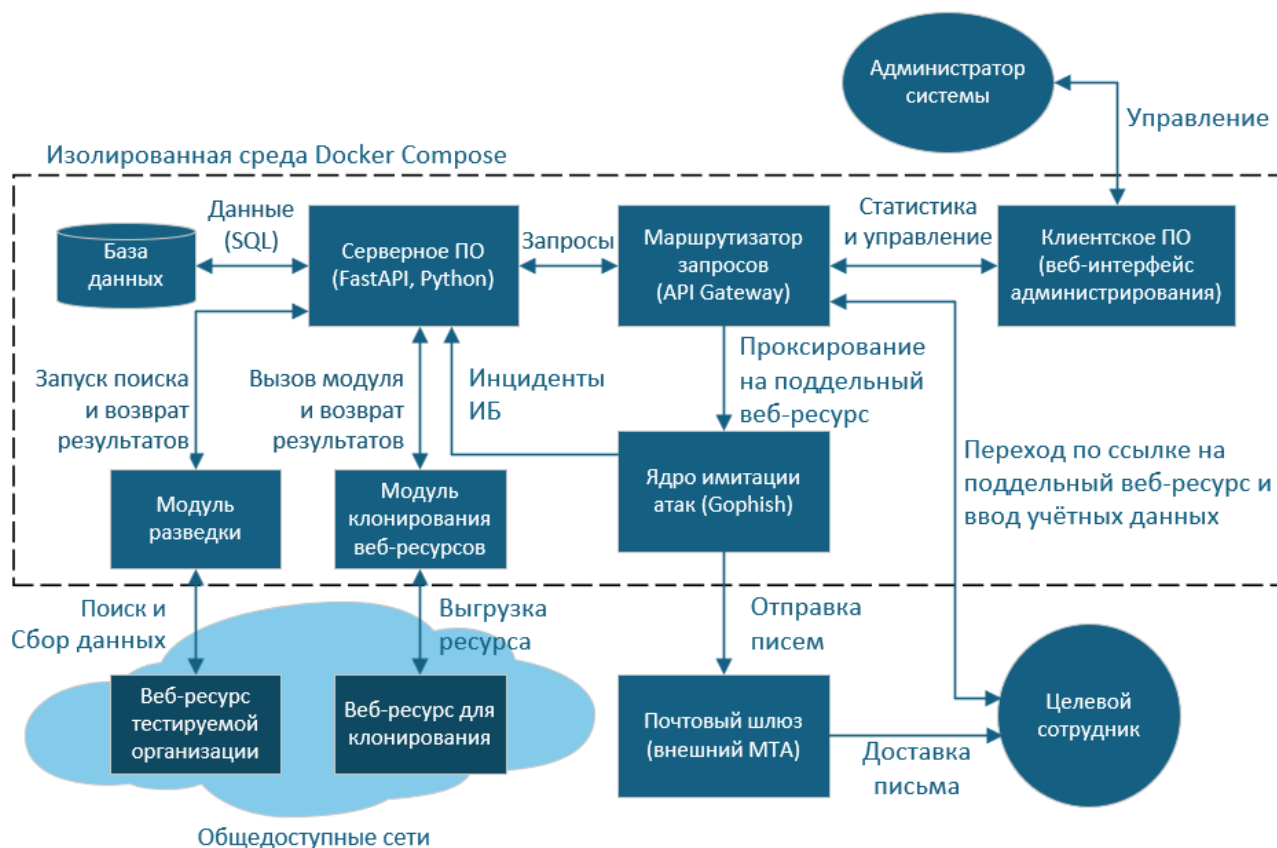
Введение

В 2025–2026 годах социальная инженерия и корпоративный фишинг остаются главными векторами кибератак на организации [1]. Создание поддельных ресурсов для кражи данных является высокоэффективным методом обхода технических средств защиты информации [2]. Противодействие угрозам требует регулярных практических тренировок персонала и превентивного анализа открытых источников [3]. Цель работы – описание архитектуры программной платформы, автоматизирующей полный цикл фишинговых аудитов.

Основная часть

Платформа использует микросервисную архитектуру в изолированной среде контейнеров. Центральным узлом выступает серверное приложение на языке Python. Общая схема архитектуры представлена на рисунке.

Внутренний маршрутизатор выполняет функцию шлюза: управляющий трафик направляется в веб-приложение, а запросы проверяемых сотрудников – на скрытый веб-сервер. Алгоритм фильтрует машинный трафик (от почтовых шлюзов и сканеров), сверяя идентификаторы браузеров и сетевые адреса с известными подсетями анализаторов. Такие автоматические переходы исключаются из итоговой оценки персонала. Реализована ролевая модель доступа к панели администрирования для защиты конфиденциальных данных.



Архитектура программного комплекса
Architecture of the software package

Для создания веб-страниц применяется модуль динамического копирования. Он загружает объектную модель сайта-источника, преобразуя относительные пути к файлам в абсолютные ссылки для корректного отображения. Модуль заменяет оригинальные формы перехватчиками и внедряет скрытые элементы отслеживания действий.

Сбор данных осуществляет модуль автоматизированной разведки. Программа-обходчик анализирует корпоративный сайт исключительно по навигационным маркерам контактов. Извлекая адреса электронной почты, алгоритм выделяет фрагмент текста (200 символов) и ищет последовательности из трех слов с прописной буквы (потенциальные ФИО). Применяя словари исключений и механизм негативного контекста, система отсеивает адреса и должности. При нахождении нескольких вариантов (потенциальных ФИО) вычисляется количество символов (дистанция) в HTML-коде до адреса электронной почты, после чего алгоритм связывает почту с ближайшим текстовым значением. Это автоматизирует формирование целевой базы.

Выполнение рассылок возложено на изолированное ядро. Оно формирует письма по шаблонам, доставляет их с подстановкой персональных данных и фиксирует этапы взаимодействия (доставка,

открытие, ввод данных), передавая события в главную базу для анализа метрик и формирования отчета.

Заключение

Разработанная платформа объединяет пассивный сбор данных, копирование ресурсов, рассылку и фильтрацию статистики. Выбранная архитектура значительно сокращает время подготовки аудитов информационной безопасности и предоставляет метрики уязвимости персонала. Дальнейшее развитие предполагает внедрение машинного обучения для обработки естественного языка, интеграцию собственного отказоустойчивого модуля отправки писем и улучшение алгоритмов копирования современных одностраничных веб-приложений.

Список использованных источников

1. Диреев И. Д. (2025) Социальная инженерия в контексте информационной безопасности. Международный научно-исследовательский журнал. (3), 39–46.
2. Гордиенко В. В., Жданов Д. М. (2024) Методы защиты от социальной инженерии и фишинга. Их достоинства и недостатки. Auditorium. (2), 45-49.
3. Туманов Е. М. (2025) Методы анализа информационной безопасности организации с использованием OSINT. Вестник науки. (5), 926–933.

References

1. Direev I. D. (2025) Social Engineering in the Context of Information Security. International Research Journal. (3), 39–46.
2. Gordienko V. V., Zhdanov D. M. (2024) Methods of Protection Against Social Engineering and Phishing. Their Advantages and Disadvantages. Auditorium. (2), 45–49.
3. Tumanov E. M. (2025) Methods of Analyzing Organization's Information Security Using OSINT. Vestnik Nauki. (5), 926–933.

Сведения об авторах

Биюмен Е.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», eugene.aether@gmail.com.

Маршалова К.Ц., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», krissmarshalova@gmail.com.

Information about the authors

Biyumen Y., student of Information Security Faculty, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, eugene.aether@gmail.com.

Marshalava K., student of Information Security Faculty, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, krissmarshalova@gmail.com.

УДК 004.56:537.531

АЛГОРИТМ АНАЛИЗА КОЛИЧЕСТВЕННЫХ СПЕКТРАЛЬНЫХ СОСТАВЛЯЮЩИХ МОЩНОСТИ СИГНАЛА ПЭМИН

И.А. Третьяков, Я.И. Рушечников, В.В. Данилов
*Донецкий государственный университет, г. Донецк,
Российская Федерация*

Аннотация. В настоящей работе проведен анализ количественных спектральных составляющих мощности сигнала, имеющего принадлежность к ПЭМИН. Показана архитектура исследовательского комплекса по поиску и анализу сигналов ПЭМИН.

Ключевые слова: ПЭМИН; электромагнитное поле; программно-определяемая радиосистема; спектральный анализ; коэффициент корреляции Пирсона.

ALGORITHM FOR ANALYZING THE QUANTITATIVE SPECTRAL COMPONENTS OF THE TEMPEST SIGNAL POWER

I.A. Tretiakov, I.A.I. Rushechnikov, V.V. Danilov
Donetsk State University, Donetsk, Russian Federation

Abstract. In this paper, an analysis of the quantitative spectral components of the signal power belonging to the TEMPEST is carried out. The architecture of a research complex for the search and analysis of TEMPEST signals is shown.

Keywords: TEMPEST; electromagnetic field; software-defined radio system; spectral analysis; Pearson correlation coefficient.

Введение

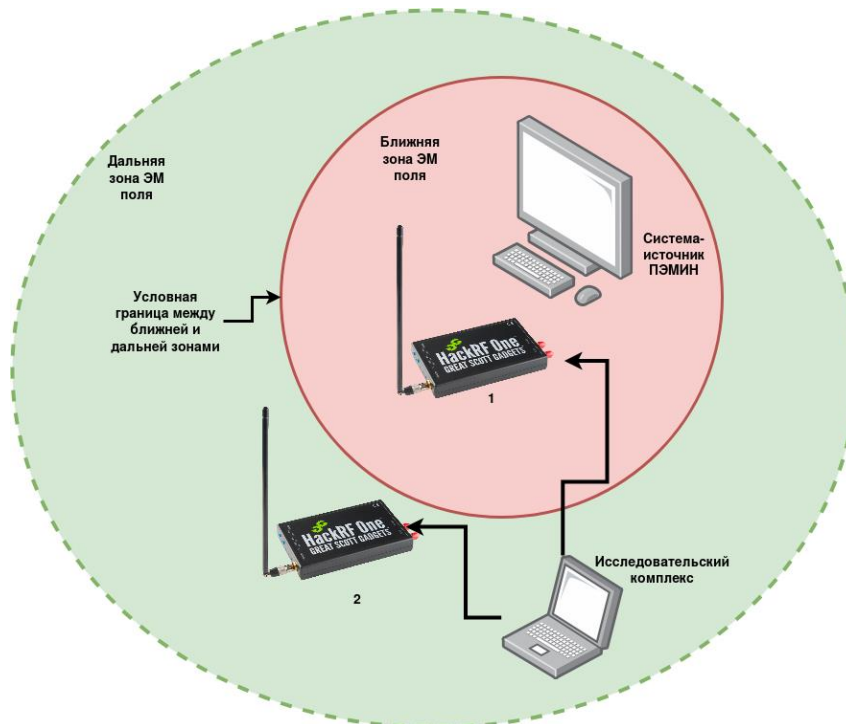
Побочные электромагнитные излучения и наводки (ПЭМИН) представляют собой совокупность спектральных компонентов, анализ которых позволяет оценить риски утечки информации из цифровых систем. В условиях возрастающей сложности электромагнитной среды исследования в этой области приобретают особую актуальность [1–3].

Основная часть

Методика эксперимента и интерпретация данных во многом определяются средой регистрации ПЭМИН. Например, при фиксации излучений в электрической сети, функционирующей как волновод, зона контроля может распространяться на десятки метров от источника утечки, включая все токопроводящие линии, в том числе цепи заземления [2].

При оценке распространения ПЭМИН через электромагнитное поле необходимо учитывать не только интерфейс передачи сигнала (например, HDMI), но также его гармоники и сложную структуру [3]. Из-за высокой сложности и многокомпонентности сигнала его прием возможен преимущественно в ближней зоне электромагнитного поля, что требует применения специализированных антенн для детектирования ПЭМИН.

Архитектура исследовательского комплекса по поиску и анализу сигналов ПЭМИН показана на рисунке.



Архитектура исследовательского комплекса по поиску и анализу сигналов ПЭМИН
Architecture of the research complex for the search and analysis of TEMPEST signals

Учитывая архитектуру, представленную на рисунке стоит отметить, что из-за сложности сигнала ПЭМИН четкое разграничение ближней и дальней зон с помощью программно-определяемых радиосистем затруднено. Однако существуют программные методы, позволяющие условно определить эти границы.

В качестве дифференцирующего алгоритма данной задачи можно использовать корреляцию Пирсона, которая представляет собой линейную зависимость между двумя массивами экспериментальных спектров. Формула для вычисления коэффициента корреляции Пирсона между массивами x и y выглядит так:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}}, \quad (1)$$

где x_i и y_i - значение элементов массивов экспериментальных данных из ближней и дальней зон соответственно; $\bar{x}$ и $\bar{y}$ - средние значения экспериментальных массивов; n - количество элементов в массиве.

Коэффициент корреляции Пирсона (1) может принимать значения от -1 до 1, где:

+1 означает полную положительную линейную зависимость;

- 1 полную отрицательную линейную зависимость;
- 0 отсутствие линейной зависимости.

Хотя коэффициент корреляции Пирсона обладает ограничениями (применим только к линейным зависимостям и имеет умеренную точность), его вычислительная эффективность и простота реализации позволяют успешно использовать его для качественной оценки спектрограмм из различных источников.

Полученные значения положительной или отрицательной корреляции дают возможность итеративно выявлять частотные участки с максимальной концентрацией ПЭМИН.

Для валидации предложенного алгоритма количественной оценки сигналов (включая ПЭМИН) было проведено исследование в УКВ-диапазоне (88-108 МГц). С целью повышения достоверности эксперимента в тестовую среду был введен контрольный источник на частоте 100 МГц, моделирующий работу радиозакладного устройства. Это позволило использовать одинаковые методики анализа как для контрольного сигнала, так и для ПЭМИН-компонентов. В результате эксперимента были получены следующие формализованные результаты:

1. Применение поэлементного дифференциального анализа экспериментальных данных с многократным усреднением для ближней и дальней зон ЭМ-поля демонстрирует ограниченную эффективность - селекция контрольного источника (100 МГц) остается слабовыраженной.

2. Введение пороговой фильтрации спектральных компонентов позволило лишь незначительно выделить аномальный пик в окрестности 100 МГц, характеризующийся немоноотонной структурой.

3. Анализ спектральной плотности мощности выявил существенное (в разы) превышение энергетических характеристик ПЭМИН-сигналов по сравнению с контрольным излучением на 100 МГц.

Заключение

Полученный результат демонстрирует значительное падение мощностных характеристик ПЭМИН при проходе через условную ближнюю границу электромагнитного поля, а размерность пространственной мощности позволяет условно судить о зоне, в рамках которой ПЭМИН будет представлять высоко вероятный технический канал утечки информации.

Список использованных источников

1. Авсентьев А. О. (2025) Модели оценки эффективности управления защитой информации от утечки по техническим каналам с применением многоагентных систем. *Вестник Воронежского института МВД России*. 1, 72-86. EDN BAUMHU.

2. Рушечников Я. И., Яновский А. В., Третьяков И. А. (2023) Программно-аппаратное обеспечение исследования электромагнитных излучений, создаваемых вычислительной техникой, в бытовой электрической сети. *Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика*. 2, 75-84. EDN LAFDGM.

3. Третьяков И. А., Рушечников Я. И., Куликова А. С., Данилов В. В. (2025) Структура аппаратных средств для восстановления информации с дисплеев. *Технические средства защиты информации: материалы XXIII МНТК*. Минск: БГУИР, 324-326. EDN WSCOKH.

References

1. Avsentev A. O. (2025) Modeli otsenki effektivnosti upravleniia zashchitoi informatsii ot utechki po tekhnicheskim kanalam s primeneniem mnogoagentnykh sistem. *Vestnik Voronezhskogo instituta MVD Rossii*. 1, 72-86 (in Russian).

2. Rushechnikov Ia. I., Ianovskii A. V., Tretiakov I. A. (2023) Programmno-apparatnoe obespechenie issledovaniia elektromagnitnykh izluchenii, sozdavaemykh vychislitelnoi tekhnikai, v bytovoi elektricheskoi seti. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: upravlenie, vychislitelnaia tekhnika i informatika*. 2, 75-84. (in Russian).

3. Tretiakov I. A., Rushechnikov Ia. I., Kulikova A. S., Danilov V. V. (2025) Struktura apparatnykh sredstv dlia vosstanovleniia informatsii s displeev. *Tekhnicheskie sredstva zashchity informatsii: materialy XXIII MNTK*. Minsk: BGUIR, 324-326 (in Russian).

Сведения об авторах

Третьяков И.А., канд. техн. наук, доц., зав. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, i.tretiakov@mail.ru.

Рушечников Я.И., ст. преп. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, ya.rushechnikov@donnu.ru.

Данилов В.В., д-р техн. наук, проф., проф. каф. радиофизики и инфокоммуникационных технологий, Донецкий государственный университет, ut5iv@mail.ru.

Information about the authors

Tretiakov I., Cand. Sci. (Tech.), Associate Professor, Head of the Department of Radiophysics and Infocommunication Technologies, Donetsk State University, i.tretiakov@mail.ru.

Rushechnikov IA., Senior Lecturer at Department of Radiophysics and Infocommunication Technologies, Donetsk State University, ya.rushechnikov@donnu.ru.

Danilov V., Dr. Sci. (Tech.), Professor, Professor at Department of Radiophysics and Infocommunication Technologies, Donetsk State University, ut5iv@mail.ru.

UDC 004.93'1

FACE RECOGNITION IN LOW LIGHT CONDITIONS

S.A.E. Al-Absi Saleh

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. This paper is devoted to an urgent problem of biometric authentication – face recognition in conditions of poor visibility and low light conditions. The article analyzes the main difficulties, such as sensory noise and loss of key image features. The Head Pose Image Database dataset was used to study the effectiveness of the algorithms. Special attention is paid to the method of expanding the training sample using data augmentation in the OpenCV library. The process of programmatically adjusting the brightness and contrast of images is described, which allows simulating extreme shooting conditions to improve the accuracy of modern computer vision systems.

Keywords: biometric authentication; low light conditions; machine learning; data augmentation,

Introduction

Authentication is one of the most effective and widely used access control mechanisms in information systems. Traditional systems use either some secret information (password) or special hardware and software keys such as smart cards, RFID cards, USB tokens, etc. for these purposes. Biometric methods of human identification and authentication are becoming more relevant every year. Facial recognition is an automated process of identifying or verifying an individual based on facial image analysis. Compared to other biometric methods, facial recognition has a number of advantages, including the absence of physical contact and the ability to be implemented using standard equipment [1]. However, despite the existence of various approaches and libraries for face recognition, the issue of recognition in conditions of poor visibility (severe weather conditions and darkness) is still relevant.

Main Part

The primary difficulty lies in the domain gap between high-quality training data and degraded real-world inputs. Dark images often suffer from sensor noise (random fluctuations in pixel values that obscure facial features), color distortion (incorrect representation of skin tones and textures), information loss (shadows often hide critical landmarks like the eyes or nose shape, making feature extraction nearly impossible for standard CNNs).

The Head Pose Image Database dataset, created by James L. Crowley, Professor Emeritus at the Polytechnic Institute of Grenoble (France), was used to study the effectiveness of detection. The database contains 2790 images of

fifteen people's faces with different angles of rotation and tilt from -90 to +90 degrees. 2 series of 93 images are available for each person. There are images with and without glasses for each person. The database was created for training and testing machine vision algorithms.

When creating a dataset to study the effectiveness of detection algorithms at different brightness and contrast values, the data augmentation technique was used. The image contrast and brightness are changed using the `cv2.convertScaleAbs(image, alpha, beta)` function. Image is the original input image, alpha is the contrast value, beta is the brightness value. Alpha values (0; 1) are used to reduce contrast. To increase – $\alpha > 1$. In this work, the alpha parameter ranged from 0 to 5 in increments of 0.1. The brightness varied in the range (-200, 200) in increments of 1. An example of the figure design and the caption to it is presented below.

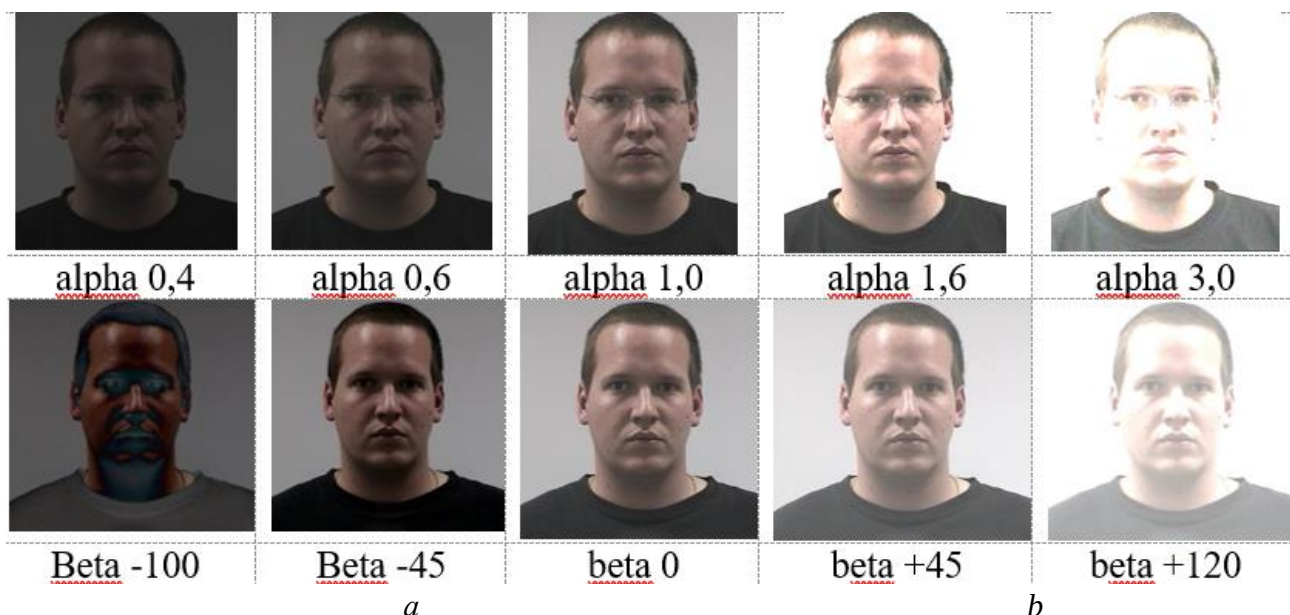


Figure capture: An example of changing brightness and contrast

The convolutional neural network showed the best detection results. Lowering the contrast ratio (alpha) by 0.7 reduced the detection accuracy, which is a predictable result. The increase in reliability only slightly increased the detection accuracy. With a significant increase in contrast ($\alpha > 3$), the detection accuracy begins to decrease. reducing the brightness level of the image reduces the accuracy of face detection faster. Increasing the brightness only slightly increased the accuracy of the detector. With a significant increase in brightness (overexposure), the detection accuracy also decreased significantly.

Conclusion

We applied the augmentation method to create a dataset for the purpose of teaching the model to detect and recognize faces in low light conditions. This makes it possible to create specialized datasets based on existing ones.

References

1. Li S. Z., Jain A. K. Handbook of Face Recognition. 3rd ed. Cham : Springer, 2024. 479 p. DOI: 10.1007/978-3-031-43366-7

Information about the authors

Al Absi Sohaib Abdo Ibrahim Saleh, master's student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, petrov@bsuir.by

UDC 004.056:004.032.26

DETECTION OF XSS ATTACKS AND SQL INJECTIONS USING CONVOLUTIONAL NEURAL NETWORKS

Qiao X., Kedo E.S

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. Cross-site scripting (XSS) and SQL injection (SQLi) remain critical threats to web application security, often bypassing traditional rule-based defenses through obfuscation techniques. This study proposes a lightweight convolutional neural network (CNN) that detects malicious inputs directly from raw HTML or script fragments using an ASCII-based grayscale representation. Evaluated on a public dataset of approximately 27,000 samples, the model achieves 98.39% accuracy with ~1 ms inference latency. The results demonstrate that compact CNN architectures can provide efficient, real-time detection of injection-based attacks in practical deployment environments.

Keywords: cross-site scripting; XSS detection; convolutional neural network; web security; intrusion detection; deep learning; HTML analysis; malicious script detection; cybersecurity.

Introduction

Web applications are frequent targets of injection attacks, among which cross-site scripting (XSS) and SQL injection (SQLi) are the most widespread. XSS allows attackers to execute malicious scripts in a user's browser, while SQLi targets backend databases by injecting crafted queries to manipulate or extract sensitive data [1, 2]. Traditional defenses, including blacklist filtering, signature-based detection, and regular expressions, are widely used in web application firewalls. However, these approaches are often ineffective against modern attack techniques that employ obfuscation, encoding, mixed-case tokens, and nested payload structures. Machine learning provides a more adaptive solution, but classical approaches rely heavily on handcrafted features and struggle to capture complex structural patterns [3]. Deep learning, particularly convolutional neural networks (CNNs), offers a promising alternative by learning directly from raw input data. This paper investigates a compact CNN model that processes ASCII-based representations of input

strings to detect injection attacks. While the primary focus is on XSS, the approach is equally applicable to SQLi patterns, as both attack types exhibit distinctive local structures such as special characters, delimiters, and repeated symbolic sequences.

Main Part

XSS and SQLi remain two of the most common vulnerabilities in modern web applications, and rule-based defenses are increasingly challenged by obfuscated payloads. While XSS enables attackers to execute malicious scripts in a user's browser, SQL injection targets backend databases by manipulating query logic to access or modify sensitive data. This paper presents a compact convolutional neural network for binary injection detection from raw HTML or script fragments. Input strings are transformed into normalized ASCII grayscale matrices, allowing the model to learn structural attack patterns directly from data. Experiments on the public Kaggle XSS dataset of about 27,000 samples show that the proposed CNN reaches 98.39% accuracy, 97.89% precision, 98.40% recall, and 98.14% F1 score on the held-out test set. The model trains in 48 s on an RTX 3080 and supports about 1 ms inference latency per sample, which makes it practical for near-real-time web security monitoring.

Traditional defenses such as blacklist filtering, signature matching, and manually maintained regular expressions are still widely used in web application firewalls. However, these methods are brittle when attackers rely on encoding tricks, mixed-case tokens, nested tags, or event-handler based payloads in XSS, as well as tautologies, UNION-based queries, and comment obfuscation in SQL injection. Classical models depend strongly on handcrafted features and may miss local spatial patterns embedded in HTML strings or query-like inputs. Recent studies have shown that deep learning is particularly effective for malicious content classification because it can learn directly from raw or weakly processed inputs. In both XSS and SQLi domains, convolution is attractive because attack payloads contain short local motifs, including tag delimiters, SQL keywords, logical operators etc.

The experiments use the public Cross-Site Scripting Dataset for Deep Learning published on Kaggle. The corpus contains approximately 27,000 labeled samples, including benign web inputs and malicious XSS payloads from reflected, stored, and DOM-related scenarios. Although the dataset primarily focuses on XSS, the proposed representation and model are generalizable to SQL injection patterns due to their shared reliance on symbolic structure and character-level anomalies. Stratified sampling is applied to split the data into 80% training and 20% testing subsets while preserving class balance. Preprocessing is intentionally simple. Each character in the raw string is converted to its ASCII code, normalized by division with 128, and written

into a fixed 100×100 matrix. Short strings are padded with zeros and long strings are truncated. This representation preserves punctuation density, tag-like shapes, SQL syntax fragments, and recurring payload patterns that are difficult to capture with word-based tokenization. The CNN model contains three convolutional blocks followed by max pooling, dropout, one dense layer, and a sigmoid output unit. ReLU activation is used after each convolution. The network is trained with binary cross-entropy loss and the Adam optimizer. Early stopping is adopted to prevent overfitting, and model quality is evaluated with accuracy, precision, recall, F1 score, and AUC-ROC.

The trained CNN converges rapidly and achieves stable validation behavior without severe overfitting. On the held-out test set, the model correctly classifies 2,362 malicious samples and 2,950 benign samples, with 38 false negatives and 50 false positives. The resulting aggregate scores are 98.39% accuracy, 97.89% precision, 98.40% recall, 98.14% F1 score, and 99.76% AUC-ROC. These results confirm that the image-style ASCII representation is sufficiently expressive for high-quality detection of injection attacks. A closer inspection of the error distribution shows that most misclassified malicious samples are heavily obfuscated strings containing nested encodings, fragmented JavaScript, or complex SQL expressions with unconventional formatting. In contrast, several false positives resemble attack payloads because they contain dense punctuation, encoded content, or debugging snippets. This behavior is acceptable for a screening model because security operations typically prefer a small surplus of alerts over missed attacks.

Computational performance is also favorable. The network contains about 1.3 million parameters, trains in 48 s on an NVIDIA RTX 3080 GPU, and produces inference latency of about 1 ms per sample. Such throughput is compatible with inline or near-inline deployment in a web application firewall, API gateway, or log triage system where fast response is required. The results show that a carefully designed CNN offers an effective trade-off between detection quality and runtime cost. Although more complex hybrid architectures can achieve even higher scores, the CNN baseline remains attractive when computational simplicity, explainability of the processing pipeline, and straightforward deployment are important design constraints.

From a practical perspective, the model can be used as a first-stage detector before deeper traffic inspection. High-confidence benign requests may pass immediately, while suspicious cases, including both XSS and SQLi, can be escalated to stricter filtering or analyst review.

Conclusion

This study demonstrates that a compact CNN combined with an ASCII-based grayscale representation can effectively detect XSS attacks and

SQL injection with high accuracy and low latency. The model captures local structural patterns in raw HTML inputs without relying on manual feature engineering. Its efficiency and strong performance make it suitable for real-time deployment in web security systems.

References

1. Nirmal K., Janet B., Kumar R. It's more than stealing cookies: exploitability of XSS. In: 2018 Second International Conference on Intelligent Computing and Control Systems. IEEE, 2018, pp. 1073-1077.
2. Rathore S., Sharma P. K., Park J. H. XSS Classifier: an efficient XSS attack detection approach based on machine learning classifier on social networking services. Journal of Information Processing Systems, 2017, 13(4), pp. 1014-1028.
3. Wang R., Jia X., Li Q., et al. Machine learning based cross-site scripting detection in online social networks. In: 2014 IEEE International Conference on High Performance Computing and Communications. IEEE, 2014, pp. 787-794.

Information about the authors

Qiao X., master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", suoyter@gmail.com.

Kedo E.S., master's student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", katyakkeda@gmail.com.

УДК 004.056:37.091.33

TELEGRAM-БОТ ДЛЯ ОБУЧЕНИЯ ПОДРОСТКОВ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ

С.Н. Петров¹, Д.В. Ермоленко², А.С. Рожкова²

¹ Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

² Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь

Аннотация. Разработаны специальные учебные сценарии, отражающие типовые ситуации в цифровой среде, связанные с безопасностью подростков, включающие попытки социальной инженерии и попытки втягивания в противоправную деятельность. Для прохождения сценариев реализован Telegram-бот. Для Telegram-бота графические материалы были адаптированы под формат мессенджера и использовались преимущественно в виде иллюстраций, эмодзи и встроенных медиаэлементов.

Ключевые слова: кибербезопасность; геймификация обучения; цифровая безопасность подростков; информационная безопасность; обучающие игровые сценарии; Telegram-бот.

TELEGRAM BOT FOR TEACHING TEENAGERS THE BASICS OF CYBERSECURITY

S.N. Petrov¹, D.V. Ermolenko², A.S. Rozhkova²

¹ *Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus*

² *Educational Institution "National Children's Technopark", Minsk, Republic of Belarus*

Abstract. Special training scenarios have been developed that reflect typical situations in the digital environment related to the safety of adolescents, including attempts at social engineering and attempts to involve them in illegal activities. A Telegram bot has been implemented to run through the scenarios. For the Telegram bot, graphic materials were adapted to the messenger format and were used primarily in the form of illustrations, emojis, and embedded media elements.

Keywords: cybersecurity; gamification of learning; digital safety of teenagers; information security; educational game scenarios; Telegram bot.

Введение

Подростки – это одно из самых активных цифровых поколений, однако при этом остаются наиболее уязвимой группой пользователей сети. Ранний доступ к интернету, высокая вовлеченность в социальные платформы и недостаточный жизненный опыт создают условия, при которых цифровые угрозы часто остаются нераспознанными. Это формирует проблему, требующую новых подходов к обучению кибербезопасности. Анализ угроз показывает, что подростки сталкиваются сразу с несколькими рисками, и их поведение в сети требует системного просвещения. Выполнен анализ образовательных приложений в области кибербезопасности, показавший, что существующие решения часто либо слишком примитивны, либо избыточно сложны [1]. Разработанный проект может занять пустующую нишу, предложив целевой аудитории (14–17 лет) контент, соответствующий их когнитивным и поведенческим условиям.

Основная часть

Реализована методика трансформации реальных угроз [2] (фишинг, вишинг, кибербуллинг, эксплуатация вредоносного ПО, AI-имперсонация, угроза деанонимизации, шантаж, вовлечение в противоправную деятельность, утечка данных, доксинг, овершеринг, сексторшен) в игровые задачи с мгновенной обратной связью, что является средством формирования навыков принятия решений в цифровой среде.

Игровая сессия проходит непосредственно в интерфейсе мессенджера. Игровой процесс построен на принципах текстового квеста и симулятора принятия решений, где каждый шаг пользователя имеет немедленное

последствие. Основным элементом взаимодействия является inline-клавиатура, прикрепленная к каждому сообщению-уровню, что обеспечивает интуитивное управление и исключает возможность ввода некорректных команд. Прогресс игрока отслеживается с помощью двух переменных: HP (Health Points) и XP (Experience Points). HP, стартующее со 100 единиц, символизирует цифровую «репутацию» или уровень защищенности. Каждая ошибка снижает HP, и при достижении нуля игра завершается, что повышает ценность каждого решения. XP, в свою очередь, начисляется за правильные ответы и служит метрикой успешности.

Сюжетная основа проходит через 75 уникальных сценариев, имитирующих реальные киберугрозы и адаптированных под формат мессенджера. Уровни сгруппированы по тематическим блокам. Игра начинается с наиболее массовых и очевидных угроз, таких как фишинг (19 сценариев) и вредоносные загрузки (5 сценариев), где от игрока требуется распознать грубые ошибки в URL или явную опасность в исполняемых файлах. По мере продвижения ситуации усложняются. Так, в блоке про мошенничество игроку предлагается оценить подлинность интернет-магазина или внезапного сбора средств от блогера.

Для поддержания вовлеченности и развития критического мышления в игру интегрировано 15 сценариев, где нет никакой угрозы. Это заставляет игрока постоянно анализировать контекст, а не действовать по заученному шаблону «все ссылки опасны». Правильное распознавание безопасной ситуации является таким же важным навыком, как и идентификация угрозы.

Кнопки выбора действий были сделаны динамическими, чтобы их названия соответствовали контексту ситуации. Вместо абстрактных «Доверять», «Проверить», «В бан», которые не всегда логичны, используются конкретные формулировки, такие как «Перейти по ссылке», «Спросить отправителя», «Заблокировать» или «Удалить». Это значительно повышает реализм и интуитивность интерфейса. Например, в сценарии с телефонным мошенничеством правильным действием будет «Сбросить», а в ситуации с угрозами в комментариях (кибербуллинг) – «Пожаловаться». Уровни про сваттинг и вовлечение в преступную деятельность демонстрируют не только цифровые, но и реальные юридические последствия неосторожных действий в сети.

В структуру бота встроена вспомогательная команда /theory, которая открывает отдельное Mini App (веб-приложение внутри Telegram) с базой знаний по вопросам кибербезопасности. Эта энциклопедия позволит игроку в любой момент изучить теорию по конкретной угрозе. Это превращает бота из простого квеста в комплексный обучающий инструмент с гибридной механикой.

Серверной часть реализована на языке Python 3.10 с использованием специализированных библиотек. Ядром системы выступает библиотека pyTelegramBotAPI (Telebot), обеспечивающая полное покрытие методов Telegram Bot API, включая работу с InlineKeyboardMarkup для реализации динамического интерфейса и WebAppInfo для интеграции мини-приложений. Для реализации веб-сервера, обслуживающего контент Mini App и обрабатывающего API-запросы, интегрирован микрофреймворк Flask.

Заключение

Разработаны специальные учебные сценарии, отражающие типовые ситуации в цифровой среде, включающие примеры фишинговых атак, попыток социальной инженерии, кибербуллинга и попытки выманить персональные данные. Для прохождения разработанных сценариев выполнили реализацию Telegram-бота, который доступен по ссылке @csgame1203bot.

Список использованных источников

1. Петров С. Н. Использование обучающих игр для формирования навыков кибербезопасности у подростков / С. Н. Петров, Д. В. Ермоленко, А. С. Рожкова // Мир студенческой науки: сборник статей X Международного научно-исследовательского конкурса. – Пенза: МЦНС «Наука и Просвещение». – 2025. – С. 7–11.
2. Солдатова, Г. У. Цифровое поколение России: компетентность и безопасность / Г. У. Солдатова, Е. И. Рассказова, Т. А. Нестик. – М. : Смысл, 2017. – 375 с.

References

1. Petrov S. N. Using educational games to develop cybersecurity skills in teenagers / S. N. Petrov, D. V. Ermolenko, A. S. Rozhkova // The World of student Science: a collection of articles from the X International Scientific Research Competition. – Penza: ICSC «Nauka i Prosveshchenie». – 2025. – P. 7–11. (in Russian).
2. Soldatova G. U. Russia's Digital Generation: competence and security / G. U. Soldatova, E. I. Rasskazova, T. A. Nestik. – M. : Smysl, 2017. – 375 p. (in Russian).

Сведения об авторах

Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.

Ермоленко Д. В., учащийся, учреждение образования «Национальный детский технопарк», chenazesm@gmail.com.

Рожкова А. С., учащийся, учреждение образования «Национальный детский технопарк», alinarazhkova@gmail.com.

Information about the authors

Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by.

Ermolenko D. V., student, Educational Institution "National Children's Technopark", chenazesm@gmail.com.

Rozhkova A. S., student, Educational Institution "National Children's Technopark", alinarazhkova@gmail.com.

УДК 004.056.5

ОРГАНИЗАЦИЯ ЦЕНТРАЛИЗОВАННОГО СБОРА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ С УЧЕТОМ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Г.С. Смотрук¹, Т.А. Пулко²

¹ООО «СофтЛайн Директ», г. Минск, Республика Беларусь

² Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрены принципы формирования централизованного контура сбора и обработки событий информационной безопасности на базе SIEM-систем с учетом требований нормативного регулирования. Особое внимание уделено реализации архитектуры сбора событий в соответствии с Приказом ОАЦ № 130, определяющим обязательный перечень регистрируемых событий. Описаны подходы к интеграции различных источников данных, включая операционные системы, базы данных, средства защиты информации и сетевое оборудование.

Ключевые слова: информационная безопасность; SIEM-систем; правила корреляции; события информационной безопасности; приказ ОАЦ №130.

IMPLEMENTATION OF CENTRALIZED COLLECTION OF INFORMATION SECURITY EVENTS IN SIEM SYSTEMS SUBJECT TO REGULATORY REQUIREMENTS

H.S. Smatruk¹, T.A. Pulko²

¹SoftLine Direct LLC, Minsk, Republic of Belarus

² Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The principles of forming a centralized circuit for collecting and processing information security events based on SIEM systems, taking into account the requirements of regulatory regulation, are considered. Special attention is paid to the implementation of the event collection architecture in accordance with OAC Order No. 130, which defines the mandatory list of recorded events. Approaches to the integration of various data sources, including operating systems, databases, information security tools, and network equipment, are described.

Keywords: information security; SIEM systems; correlation rules; information security events; OAC Order No. 130.

Введение

Для формирования целостной картины состояния информационной безопасности используются системы класса SIEM (Security Information and Event Management), обеспечивающие централизованный сбор, нормализацию, хранение и анализ событий информационной безопасности от различных источников. Принятие приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» установило обязательный перечень типов и записей событий информационной безопасности, подлежащих регистрации, консолидации и хранению. Данный перечень фактически определяет минимально необходимый набор наблюдаемых событий для мониторинга состояния информационной безопасности и создает нормативную основу для построения процессов выявления и расследования инцидентов.

Средства защиты информации, включая антивирусные решения, системы обнаружения и предотвращения вторжений, системы предотвращения утечек данных, средства управления привилегированным доступом, сканеры уязвимостей, системы динамического анализа и изоляции подозрительных объектов, платформы автоматизации реагирования и оркестрации безопасности, а также системы мониторинга, формируют отдельный поток событий, имеющий критическое значение для мониторинга состояния безопасности. Как правило, журналы таких систем концентрируются на сервере администрирования, откуда передаются в SIEM по протоколу Syslog либо через специализированные агентские модули. Регистрируемые события включают обнаружение и блокирование вредоносных объектов, выявление уязвимостей и результатов сканирования, изменение конфигурации средств защиты, запуск и остановку сервисов, выполнение автоматизированных сценариев реагирования, а также действия администраторов. Контроль этих событий позволяет не только выявлять атаки, но и отслеживать корректность функционирования самих средств защиты и факты их возможного обхода или отключения. Интеграция прикладного программного обеспечения и средств защиты информации в SIEM-систему реализуется с использованием комбинации агентского сбора, парсинга файлов журналов и подключения через программные интерфейсы. Такой подход обеспечивает полноту охвата событий, соответствие нормативным требованиям и формирует единое информационное пространство для последующей корреляции и выявления инцидентов информационной безопасности.

Основная часть

Для организации вышеописанного решения реализован комплексный и нормативно обоснованный контур сбора событий информационной безопасности, охватывающий все основные классы источников, определенные требованиями Приказа ОАЦ при Президенте Республики Беларусь от 25.07.2023 № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». Архитектура сбора включает централизованную пересылку событий операционных систем Windows с использованием серверов Windows Event Collector, прямое агентское подключение для критически значимых серверов, а также применение встроенных механизмов аудита и системных журналов в операционных системах Linux с маршрутизацией данных через syslog-транспорт.

Аудит систем управления базами данных организован посредством специализированных коннекторов, обеспечивающих извлечение событий непосредственно из системных таблиц и представлений аудита, что позволяет фиксировать контроль сессий, действия пользователей с административными привилегиями и операции управления правами доступа. Для телекоммуникационного оборудования, межсетевых экранов, прикладного программного обеспечения и средств защиты информации используется унифицированный механизм передачи событий по протоколу Syslog либо через агентские модули с последующей нормализацией и классификацией в SIEM-системе.

Ключевым техническим аспектом такого решения является обеспечение гарантированной доставки событий. Это достигается за счет локальной буферизации на агентах, использования очередей сообщений и дисковых очередей syslog-сервисов, а также применения промежуточных коллекторов, что минимизирует риск потери данных при пиковых нагрузках и временных отказах каналов связи. Такой подход обеспечивает формирование устойчивого, воспроизводимого и полноформатного потока событий информационной безопасности, соответствующего нормативным требованиям и особенностям инфраструктуры организации. Данная база событий служит основой для разработки и апробации правил корреляции, направленных на выявление инцидентов и угроз информационной безопасности.

Практическая значимость реализации указанного подхода заключается в возможности использования разработанного набора правил корреляции при внедрении и эксплуатации систем мониторинга информационной безопасности в организациях, обязанных выполнять требования Приказа ОАЦ № 130, а также при модернизации существующих систем централизованного сбора и анализа событий информационной безопасности.

Заключение

Продемонстрирован комплексный подход к построению контура централизованного сбора событий информационной безопасности, ориентированный на соответствие требованиям нормативного регулирования и практическим задачам мониторинга. В качестве методологической основы использованы положения Приказа ОАЦ № 130, определяющего минимально необходимый набор регистрируемых событий и тем самым задающего формализованную модель наблюдаемости информационной инфраструктуры. Показано, что сформированный контур является основой для последующей корреляции и выявления инцидентов, а также соответствует требованиям к построению систем мониторинга безопасности.

Сведения об авторах

Смотрук Г.С., инженер-системотехник, ООО «СофтЛайн Директ», smotrukgerman@gmail.com.

Пулко Т.А., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pulko@bsuir.by

Information about the authors

Smatruk H.S., system engineer, SoftLine Direct LLC, smotrukgerman@gmail.com.

Pulko T.A., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pulko@bsuir.by.

УДК 004.056.5:004.414.3

АВТОМАТИЗИРОВАННЫЙ СТАТИЧЕСКИЙ АНАЛИЗ УЯЗВИМОСТЕЙ МЕССЕНДЖЕРА PEREGRINE С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

С.Н. Петров¹, Е.С. Пакуль², А.А. Корчинский²

¹ Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

² Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь

Аннотация. Разработан мессенджер имеет клиент-серверную архитектуру и использующий национальные стандарты шифрования. Выполнено статическое тестирование исходного кода мессенджера на уязвимости с использованием сканер L3X и больших языковых моделей для валидации результатов, полученных от сканера. Такой подход позволил отфильтровать до 85% ложноположительных срабатываний.

Ключевые слова: системы обмена мгновенными сообщениями, мессенджеры, сквозное шифрование, информационная безопасность, криптографические протоколы, тестирование программного обеспечения.

AUTOMATED STATIC VULNERABILITY ANALYSIS OF THE PEREGRINE MESSENGER WITH LARGE LANGUAGE MODELS

S.N. Petrov¹, Y.S. Pakul², A.A. Korchinsky²

¹ *Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus*

² *Educational Institution “National Children’s Technopark”, Minsk, Republic of Belarus*

Abstract. The developed messenger has a client-server architecture and uses national encryption standards. Static testing of the messenger's source code for vulnerabilities was performed using the L3X scanner and large language models to validate the results obtained from the scanner. This approach allowed filtering out up to 85% of false positives.

Keywords: instant messaging systems, instant messengers, end-to-end encryption, information security, cryptographic protocols, software testing.

Введение

Мессенджеры стали универсальным инструментом для коммуникации и совместной работы. Однако в связи с актуализацией проблематики обеспечения безопасности данных при их передаче и возможными ограничениями (например, запретом на использование) становятся актуальными вопросы разработки альтернативных, безопасных мессенджеров. Целью проекта является создание безопасного мессенджера на языке программирования Rust с защитой пользовательских данных и end-to-end (сквозным) шифрованием на основе национальных криптографических стандартов. При разработке защищенного мессенджера большое внимание было уделено вопросам тестирования продукта. В частности, выполнено статическое тестирование исходного кода мессенджера на наличие уязвимостей.

Основная часть

Разработанный мессенджер имеет клиент-серверную архитектуру, в которой клиенты взаимодействуют с центральным сервером, пересылающим сообщения от отправителя к получателю, выполняющим аутентификацию пользователей и управление доступом. Основной акцент в проекте сделан на безопасность. Центральным звеном стала разработка библиотеки bee2-rs на языке программирования Rust. Библиотека создана для вызовов функций библиотеки Bee2, написанной на языке программирования C.

У статических анализаторов есть особенность – большое количество ложноположительных результатов. Из-за того, что большинство анализаторов используют регулярные выражения или похожие способы анализа исходного текста, возникает сложность обработки и интерпретации полученных результатов. Отсюда возникла идея – использовать статические анализаторы кода, которые основываются на регулярных выражениях, а после использовать большие языковые модели (LLM) для валидации результатов.

Был проведен статический анализ кода мессенджера с использованием статического анализатора L3X (L3X AI-driven Static Analyzer). С кодом проекта можно ознакомиться в репозитории Github по ссылке <https://github.com/VulnPlanet/l3x>. В данном проекте разработчиками была заложена идея использования валидации результатов сканирования с использованием трех языковых моделей по принципу мажоритарного голосования. Однако на данный момент ими реализована поддержка только облачного API ChatGPT, что создавало риски конфиденциальности и зависимость от внешних сервисов. Для решения этой проблемы авторами была выполнена существенная модификация сканера L3X, а именно осуществлен переход на локальные большие языковые модели Gemma 3 12B, Qwen 3 14B, Phi-4 Reasoning Plus 15B.

Паттерны, используемые для поиска уязвимостей, были разделены на три категории по степени критичности: High, Medium и Low. Категория High относится к критическим уязвимостям. Например, уязвимости в блоке unsafe или использование неинициализированной памяти категоризируется как High. В результате сканирования без валидации было обнаружено 1537 уязвимостей, включая 103 High, 1292 Medium и 190 Low уязвимостей. В дальнейшем были использованы большие языковые модели для валидации результатов. Такой подход доказал свою эффективность в значительном снижении уровня ложноположительных срабатываний по сравнению с исходным сканированием только инструментом l3x без использования LLM в качестве валидаторов (до 85% ложноположительных результатов).

Языковая модель Gemma 3 12B подтвердила 6 High, 211 Medium и 7 Low уязвимостей. Однако все 6 High уязвимостей были проверены вручную, и ни одна из них не представляла опасности. Проверки остальных потенциальных уязвимостей также показали отсутствие рисков.

Языковая модель Qwen 3 14B подтвердила 51 High уязвимостей, 119 Medium, 85 Low, 1219 False Positive, 63 Unknown. False positive rate составил 83.409%. Из 51 High уязвимости, снова ни одна из них не представляет опасности. В этот раз одна уязвимость была про выделение памяти в коде серверной части, основанное на непроверенном значении,

однако несколькими строками кода выше в той же функции проверка на максимальный размер данных все же осуществляется. Одна уязвимость была про возможное неправильное использование потоков и синхронизации, однако в том же файле для всех данных, которые могут быть получены/изменены в нескольких потоках, использовался тип данных, предотвращающий одновременные чтение или запись с нескольких потоков.

Языковая модель Phi 4 Reasoning Plus (15B) подтвердила 0 High, 0 Medium, 0 Low, 1395 False Positive, 142 Unknown. False positive rate составил 100%. Вероятнее всего это означает, что модель Phi 4 Reasoning Plus не подходит для анализа уязвимостей программного кода.

Заключение

Общий объем написанного кода составил 10452 строк, из которых 7860 строк составляет код мессенджера и 2592 строки составляет код библиотеки bee2-rs. С исходным кодом мессенджера (серверная и клиентская часть, библиотека bee2-rs) можно ознакомиться в репозитории Github по ссылке <https://github.com/tpyauheni/peregrine>. Был проведен статический анализ кода мессенджера с использованием статического анализатора L3X и больших языковых моделей. Такой подход доказал свою эффективность в значительном снижении уровня ложноположительных срабатываний (до 85%) по сравнению со сканированием только инструментом L3X.

Сведения об авторах

Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.

Пакуль Е. С., учащийся, учреждение образования «Национальный детский технопарк», eduartpastado@gmail.com.

Корчинский А. А., учащийся, учреждение образования «Национальный детский технопарк», ak47reborntumpa@gmail.com.

Information about the authors

Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Belarusian State University of Informatics and Radioelectronics, petrov@bsuir.by.

Pakul Y. S., student, Educational Institution "National Children's Technopark", eduartpastado@gmail.com.

Korchinsky A. A., student, Educational Institution "National Children's Technopark", ak47reborntumpa@gmail.com.

УДК 004.056:004.65

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИЩЕННОЙ ОБРАБОТКИ СЛУЖЕБНОЙ ИНФОРМАЦИИ ДЛЯ ОРГАНОВ ПОГРАНИЧНОЙ СЛУЖБЫ

А.А. Фирсов, А.С. Герасимов

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Рассматривается проблема обеспечения конфиденциальности, целостности и доступности служебной информации в деятельности органов пограничной службы. Предлагается архитектура автоматизированной системы «Поиск», реализующая многоуровневое разграничение доступа на основе иерархической модели и двухконтурный механизм поиска данных. Приводятся результаты тестирования системы, подтверждающие эффективность предложенных методов защиты информации.

Ключевые слова: защита информации; разграничение доступа; автоматизированная система; пограничная служба; конфиденциальность; целостность данных; веб-приложение; база данных.

AUTOMATED SYSTEM FOR SECURE PROCESSING OF OFFICIAL INFORMATION FOR THE BORDER GUARD SERVICE

A.A. Firsov, A.S. Gerasimov

*Educational Institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. The problem of ensuring confidentiality, integrity and availability of official information in the activities of border guard agencies is considered. The architecture of the automated system «Poisk» is proposed, which implements multi-level access control based on a hierarchical model and a dual-circuit data search mechanism. The results of system testing are presented, confirming the effectiveness of the proposed methods of information protection.

Keywords: information security; access control; automated system; border guard service; confidentiality; data integrity; web application; database.

Введение

Современная оперативная деятельность органов пограничной службы характеризуется использованием разрозненных источников информации (бумажные носители, локальные электронные файлы, ведомственные базы данных), что приводит к нарушению трех базовых принципов защиты информации: конфиденциальности (несанкционированный доступ к данным), целостности (дублирование и искажение информации) и доступности (значительные временные затраты на поиск). Как

отмечается в исследованиях, посвященных автоматизации деятельности органов правопорядка, подобная фрагментация данных является типичной проблемой ведомственных структур, требующей системного решения [1]. Отсутствие единой централизованной системы создает предпосылки для утраты или компрометации служебных сведений, что недопустимо в деятельности органов государственного управления.

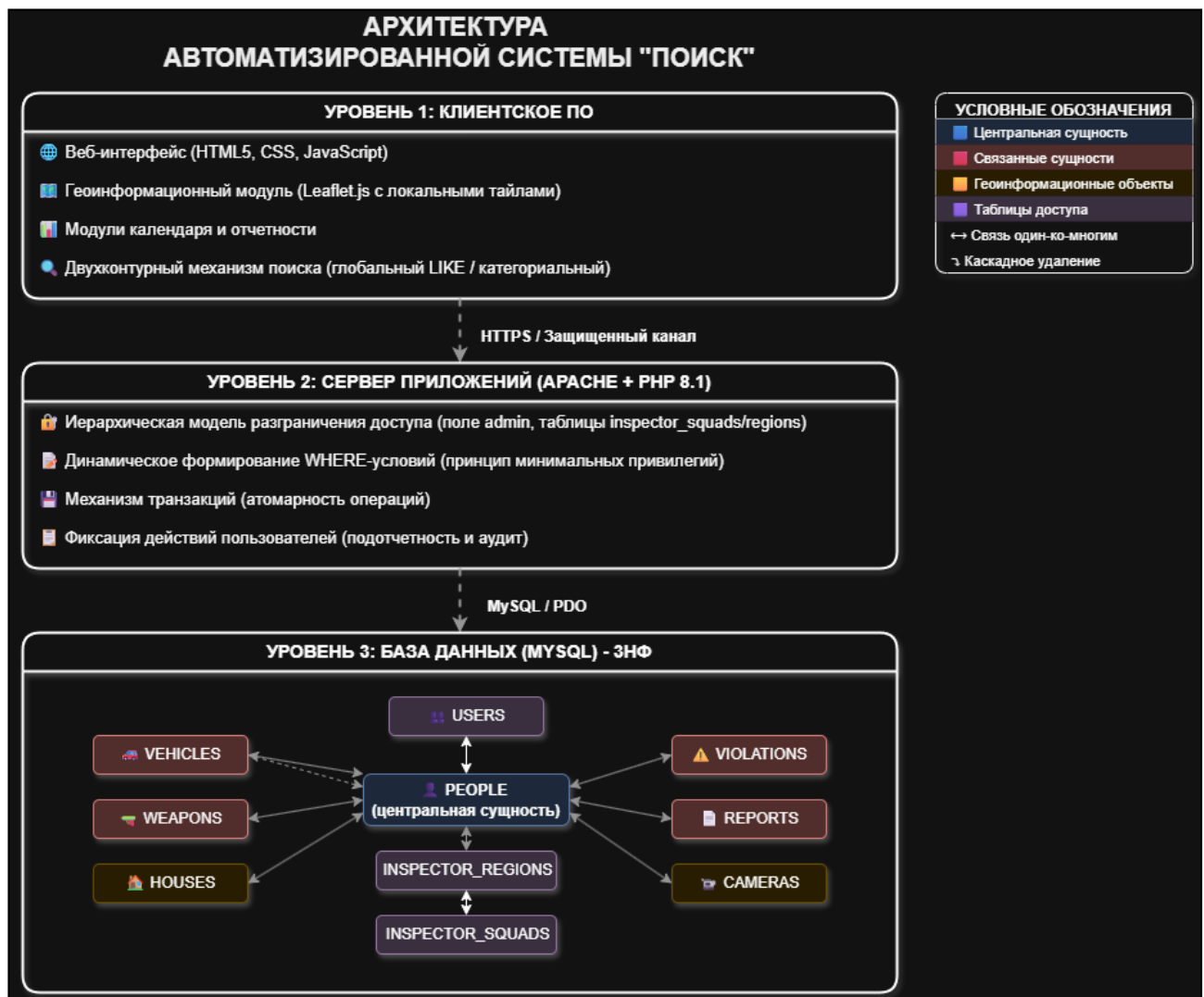
Целью работы является проектирование и разработка автоматизированной системы «Поиск», обеспечивающей защищенную обработку служебной информации должностными лицами пограничных подразделений.

Основная часть

Архитектура проектируемой системы построена по трехуровневому принципу «клиент-сервер» (рис. 1) с использованием технологического стека Apache, MySQL, PHP 8.1. Такой подход обеспечивает централизованное хранение данных на защищенном сервере и исключает риски утраты информации при повреждении клиентского оборудования

Ключевым механизмом обеспечения конфиденциальности является иерархическая модель разграничения доступа, реализованная через поле `admin` в таблице пользователей и таблицы связей `inspector_squads` и `inspector_regions`. Разработанная модель развивает известные подходы к управлению доступом в ведомственных информационных системах [2] и адаптирует их к специфике пограничной службы. Модель включает шесть уровней привилегий – от рядового инспектора до системного администратора. При выполнении любого SQL-запроса система динамически формирует условия `WHERE` на основе территориальной принадлежности пользователя, что гарантирует доступ только к данным в пределах зоны ответственности. Данный подход реализует принцип минимально необходимых привилегий и предотвращает утечки конфиденциальной информации.

Целостность данных обеспечивается нормализованной реляционной схемой базы данных (третья нормальная форма) с системой внешних ключей и каскадных операций. Центральной сущностью является таблица `people`, связанная отношениями с таблицами транспортных средств (`vehicles`), оружия (`weapons`), правонарушений (`violations`) и отчетов (`reports`). Механизм транзакций MySQL гарантирует атомарность операций при изменении связанных данных, что исключает возникновение противоречивого состояния базы.



Архитектура автоматизированной системы «Поиск»
Architecture of the automated system "Poisk"

Для обеспечения доступности информации разработан двухконтурный механизм поиска. Первый контур (глобальный поиск) выполняет параллельные запросы с оператором LIKE ко всем текстовым полям девяти основных таблиц, обеспечивая оперативное получение результатов по неструктурированному запросу. Второй контур (категориальный поиск) позволяет формировать структурированные выборки путем последовательного выбора территориальных фильтров и категорий оперативного учета, что оптимизировано для аналитической работы.

Геоинформационный модуль, реализованный на базе библиотеки Leaflet.js с использованием локально хранящихся тайлов, обеспечивает визуализацию пространственных данных (жилые дома, камеры видеонаблюдения) в условиях отсутствия стабильного интернет-соединения, что критически важно для полевых условий работы.

Модуль поддерживает фильтрацию объектов по типам и контекстный переход к полным карточкам учета.

Модули календаря и отчетности интегрированы в единую систему планирования и документирования оперативно-служебной деятельности. Каждый отчет привязывается к конкретному физическому лицу с фиксацией времени создания и автора, что обеспечивает подотчетность и возможность аудита всех действий пользователей.

Заключение

Таким образом, разработанная автоматизированная система «Поиск» представляет собой комплексное техническое средство защиты информации, обеспечивающее конфиденциальность (через иерархическое разграничение доступа, реализованное с учетом современных подходов [2]), целостность (через нормализованную структуру данных) и доступность (через оптимизированные механизмы поиска) служебной информации в деятельности органов пограничной службы.

Список использованных источников

1. Петров В.И., Сидоров А.А. (2021) Информационные технологии в управлении органами правопорядка. Вестник БГУИР. № 4 (58). С. 45–52.
2. Кузнецов А.В., Морозов П.П. (2023) Модели разграничения доступа в ведомственных информационных системах. Информационная безопасность. № 3. С. 23–29.

References

1. Petrov V.I., Sidorov A.A. (2021) Information Technologies in Law Enforcement Management. Proceedings of BSUIR. No. 4 (58). pp. 45–52 (in Russian).
2. Kuznetsov A.V., Morozov P.P. (2023) Access Control Models in Departmental Information Systems. Information Security. No. 3. pp. 23–29 (in Russian).

Сведения об авторах

Фирсов А.А., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», andrey2017firsov@gmail.com.

Герасимов А.С., магистр, старший преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.gerasimov@bsuir.by.

Information about the authors

Firsov A.A., cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, andrey2017firsov@gmail.com

Gerasimov A.S., Master, Senior Lecturer, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.gerasimov@bsuir.by

УДК 004.056.5

МЕТОД ЗАЩИТЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ГЕНЕРАЦИИ ЛОЖНЫХ СЕКРЕТОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

И.А.Лепесий, Е.С.Романович

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В работе предложен метод защиты криптографических ключей на основе внедрения ложных сегментов, сгенерированных с помощью машинного обучения. Традиционные методы защиты часто неприменимы в облачных системах. Схема включает разделение ключа, генерацию ложных сегментов через генеративно-состязательные сети и их перемешивание. Использование машинного обучения обеспечивает правдоподобное распределение битов. Это усложняет задачу злоумышленника при компрометации хранилища, делая перебор комбинаций сегментов вычислительно нецелесообразным из-за экспоненциального роста числа ложных вариантов.

Ключевые слова: криптография; криптографическая защита; AES-256; разделение ключа; машинное обучение; медовое шифрование; разделение секрета; генеративно-состязательные сети; ложные данные; информационная безопасность.

METHOD OF PROTECTING CRYPTOGRAPHIC KEYS BASED ON GENERATION OF FALSE SECRETS USING MACHINE LEARNING

I.A. Lepesy, E.S. Romanovich

*Educational Institution "Belarusian State University of Informatic and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. This paper proposes a method for protecting cryptographic keys based on the embedding of false segments generated using machine learning. Traditional security methods are often inapplicable to cloud systems. The scheme involves key splitting, generating false segments using generative adversarial networks, and shuffling them. Machine learning ensures a plausible bit distribution. This complicates the attacker's task when compromising the storage, making brute-force segment combinations computationally infeasible due to the exponential growth of false combinations.

Keywords: cryptography; cryptographic protection; AES-256; key splitting; machine learning; honey encryption; secret sharing; generative adversarial networks; decoy data; information security.

Введение

В современных условиях цифровой трансформации криптографические алгоритмы, такие как AES-256, обеспечивают надежную защиту данных при передаче и хранении. Однако безопасность системы часто определяется не стойкостью алгоритма шифрования, а защищенностью ключевой информации. Инциденты, связанные

с утечкой баз данных, приводят к тому, что злоумышленник получает доступ к зашифрованным ключам или их компонентам.

Основная часть

Традиционные методы защиты, такие как аппаратные модули безопасности или доверенные исполняющие среды, не всегда применимы в распределенных облачных системах из-за высокой стоимости и сложности интеграции. Альтернативным подходом является концепция «медового шифрования», предполагающая наличие ложных данных, которые выглядят правдоподобно для атакующего. И в создании этих ключей может помочь машинное обучение (далее – МО)

Предлагаемая схема защиты включает три основных этапа:

1. Разделение ключа. Ключ шифрования K длиной 256 бит разделяется на m сегментов (например, $m=3$) с использованием схемы разделения секрета или побайтового распределения.

2. Генерация ложных сегментов. Для каждого реального сегмента генерируется n ложных сегментов. Критически важно, чтобы распределение битов в ложных сегментах соответствовало распределению в реальных ключах.

3. Перемешивание и хранение. Реальные и ложные сегменты перемешиваются и сохраняются в хранилище. Метаданные, указывающие на принадлежность сегмента к реальному ключу, не хранятся явно, а восстанавливаются только при успешной аутентификации пользователя.

Для генерации ложных сегментов оптимально использовать генеративно-состязательной сети. Архитектура включает: генератор – принимает на вход случайный шум z и выдает вектор битов длиной 85 бит (при разделении 256 бит на 3 части). Дискриминатор: Обучается различать реальные сегменты ключей) и сгенерированные векторы.

Заключение

В работе предложен метод защиты криптографических ключей, основанный на внедрении ложных сегментов, сгенерированных с помощью машинного обучения. Использование МО в криптографии огромный потенциал в помощи криптографу. Это усложняет задачу злоумышленника при компрометации хранилища ключей, так как перебор комбинаций сегментов становится вычислительно нецелесообразным из-за экспоненциального роста числа ложных вариантов.

Список использованных источников

1. Алпайдин, Э. Машинное обучение: новый искусственный интеллект / Э. Алпайдин. – М. : Альпина Паблишер, 2017. – 208 с.
2. Основы криптографии / А. П. Алфёров [и др.]. – М. : Гелиос АРВ, 2005. – 430 с.

References

1. Alpaidin, E. Machine Learning: A New Artificial Intelligence / E. Alpaidin. – Moscow : Alpina Publisher, 2017. – 208 p.
2. Fundamentals of Cryptography / A. P. Alfyorov [et al.]. – Moscow : Helios ARV, 2005. – 430 p.

Сведения об авторах

Романович Е.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», egor.romanovich.00@inbox.ru

Лепесий И.А., маг. воен. наук, старший преподаватель кафедры тактической и общевойсковой подготовки, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», dljatebja1@mail.ru

Information about the authors

Romanovich E., cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, egor.romanovich.00@inbox.ru

Lepesiy I., Master of Military Sciences, Senior Lecturer, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, dljateb-ja1@mail.ru

UDC 004.7.056.5

DETECTING CYBER-ATTACKS BASED ON NETWORK STEGANOGRAPHY

¹Duong Ngoc Anh, ²Dao Thanh Huong

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Annotation: With the rapid development of information technology and the growing number of network attacks, ensuring the security of computer networks is particularly important. One of the covert methods of data transmission is network steganography, which allows information to be embedded in legitimate network traffic. Such approaches are used by attackers to control malware, establish covert communication channels, and leak confidential data. This paper examines the main attack methods based on network steganography and analyzes modern approaches to their detection.

Keywords: network steganography; covert channel detection; steganalysis; information hiding; machine learning; deep learning; multilayer hybrid detection; Zero Trust.

Introduction

Network steganography is a type of steganography that uses network protocols of the Open Systems Interconnection (OSI) reference model as carriers of secret data. Generally, network steganography is a family of methods for modifying data in network protocol headers and packet payload fields, altering the structure of packet transmission, and using hybrid methods within a particular network protocol (sometimes several at once) [1].

The fundamental principle of network steganography is to utilize inherent features of network communication in order to transmit information without raising suspicion. These techniques can involve modifying protocol fields, manipulating packet payloads, or altering temporal characteristics such as inter-packet delays. As a result, network steganography enables attackers to bypass traditional security mechanisms, making it a critical challenge in the field of cybersecurity.

Main part

Network steganography methods can be classified according to how they modify protocol data units (PDUs), and are generally divided into two main categories: intra-protocol techniques and inter-protocol techniques. Intra-protocol methods operate within a single protocol and can be grouped into three main approaches: modifying protocol PDU fields, hybrid methods, and modifying PDU timing relationships. These approaches include techniques such as payload embedding (e.g., DNS tunneling), protocol header manipulation (e.g., IP, TCP, SCTP fields), and timing-based strategies such as packet reordering, intentional packet loss, or delay alteration. In contrast, inter-protocol methods exploit the interaction between multiple protocols, with PadSteg being a prime example.

To clarify further, here are some specific examples:

1. Payload-based methods. They embed hidden data directly into packet payloads. A common example is DNS tunneling, where data is encoded within domain names in DNS queries, enabling covert data transmission through legitimate traffic. Another approach involves modifying the least significant bits of application-layer data (e.g., HTTP or VoIP), making the changes difficult to detect.

2. Protocol-based methods. Protocol-based techniques modify fields within network protocol headers, often using unused or optional fields in IP, TCP, or UDP. For example, HICCUPS introduces intentional checksum errors in wireless networks to transmit hidden data, which can only be decoded by specific receivers. Similarly, PadSteg uses Ethernet frame padding to carry covert information, as these fields are typically ignored.

3. Timing-based methods. These methods encode information by altering packet timing rather than content. The LACK method delays selected VoIP packets so they appear lost to normal receivers but are used by covert ones. In TCP packet dropping signaling, packet loss patterns represent data. Another technique modifies inter-PDU delays, where different time intervals correspond to encoded information.

Given the diversity of network steganography techniques, no single detection method can address all threats. Each approach – whether signature-based, anomaly-based, machine learning-driven, or active defense – offers distinct advantages while suffering from specific limitations. Signature-based methods provide reliable detection of known attacks but cannot identify novel variants. Anomaly-based techniques can uncover unknown threats yet generate high false positive rates. Machine learning and deep learning achieve impressive accuracy but demand substantial data and computational resources. Multilayer approaches balance these trade-offs at the cost of architectural complexity, while active defense mechanisms prevent attacks proactively but may impact network performance.

A comparative understanding of these approaches is therefore essential for selecting appropriate countermeasures. As steganographic attacks continue to evolve in sophistication, understanding the trade-offs between different detection methods becomes increasingly crucial. Table provides a structured comparison of the approaches discussed in this paper, summarizing fundamental principles of network steganography detection methods.

Comparison of Network Steganography Detection Approaches

Approach	Main Methods	Fundamental Principle	Strengths	Limitations
Signature-based Detection	Pattern matching. Detection of traces from known steganography tools	Relies on a database of signatures extracted from known hiding techniques	Simple implementation. High accuracy for known attacks	Unable to detect novel/zero-day attacks. Requires frequent signature updates
Anomaly-based Detection	Statistical analysis (entropy, frequency). Inter-packet delay analysis. Detection of abnormal header values	Establishes baseline of normal protocol behavior and identifies deviations	Capable of detecting unknown attacks. Independent of signature databases	High false positive rate. Difficult to determine optimal thresholds

Completing the table

Approach	Main Methods	Fundamental Principle	Strengths	Limitations
Machine Learning Detection	Supervised learning (Random Forest, SVM). Unsupervised learning (Clustering)	Trains classification models on labeled datasets to distinguish malicious traffic	Automates detection process. Adaptable to various attack types	Requires large, high-quality training data. Limited interpretability ("black box" issue)
Deep Learning Detection	Convolutional Neural Networks (CNN). Recurrent Neural Networks (RNN/LSTM)	Automatically extracts hierarchical features from raw data to detect complex patterns	Highest detection accuracy. Eliminates manual feature engineering	High computational resource demands. Requires massive amounts of training data
Multilayer/Hybrid Detection	Combination of multiple techniques. Selective analysis based on suspicion level	Performs lightweight analysis at upper layers, triggers deep inspection only when anomalies are detected	Optimizes system performance. Balances accuracy and processing speed	Complex architectural design. Challenging parameter optimization
Active Defense (Wardens)	Packet normalization. Overwriting unused/reserved header fields	Proactively sanitizes packets to destroy hidden data before reaching destination	Complete prevention capability. No detection required	May degrade network performance. Cannot distinguish sophisticated attacks

Conclusion

This paper has presented a comprehensive overview of detection methods for network steganography-based cyber attacks. The comparative analysis reveals that each approach possesses distinct strengths and limitations. Signature-based detection offers simplicity and high accuracy for known attacks but fails to identify novel threats. Anomaly-based detection can uncover unknown variants yet suffers from high false positive rates and threshold configuration challenges. Machine learning and deep learning techniques achieve superior accuracy through automated feature extraction; however, they

demand substantial computational resources and large, high-quality training datasets.

For practical deployment in real-world environments, multilayer/hybrid detection emerges as the most promising direction. By combining multiple detection layers with increasing complexity, this approach effectively balances detection accuracy, processing speed, and resource utilization – critical factors for operational network infrastructures. Furthermore, the continued advancement of artificial intelligence and deep learning will remain central to enhancing detection capabilities against increasingly sophisticated steganographic techniques.

Notably, as traditional network perimeters continue to dissolve, the Zero Trust model – with its core principle of "never trust, always verify" – becomes increasingly relevant. Zero Trust architecture mandates inspection of every packet and data stream regardless of origin, enabling the discovery of even the most concealed covert channels. The integration of advanced detection techniques within a Zero Trust framework creates a robust defense mechanism, protecting systems against the growing threat landscape of steganography-based attacks.

References

1. Peskova O.Yu., Khalaburda G.Yu. Application of network steganography to conceal data transmitted over communication channels // Bulletin of the Southern Federal University. Technical Sciences, 2012. – T. 137. – № 12 (137). – C. 167-176.
2. N. Singh, J. Bhardwaj, and G. Raghav. Network Steganography and its Techniques: A Survey, International Journal of Computer Applications, vol. 174, no. 2, pp. 30-35, Sep. 2017. [Electronic resource].
3. Badar, L. T., Carminati, B., & Ferrari, E. (2025). A comprehensive survey on stegomalware detection in digital media, research challenges and future directions. Signal Processing, 231, 109888.

Information about the authors

Duong N.A., student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", dngocanh2412@gmail.com.

Dao T.H., student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", daothanhuong2k3ad@gmail.com.

УДК 004.056.5

ПРИМЕНЕНИЕ СХЕМ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

С. С. Скапцов, М. А. Кисель

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье исследуются вопросы обеспечения конфиденциальности при обработке данных в облачных средах с использованием технологии полностью гомоморфного шифрования. Данный метод позволяет выполнять математические операции над зашифрованными данными без их дешифрации на стороне сервера. Проведен анализ современных схем BFV и CKKS, рассмотрены механизмы накопления шума в шифротекстах и предложена модель защищенного взаимодействия, минимизирующая риски утечки информации на этапе вычислений.

Ключевые слова: криптография, гомоморфное шифрование, облачные вычисления, конфиденциальность данных, информационная безопасность, шифротекст, схема CKKS, вычислительная сложность, защита информации, алгоритм.

APPLICATION OF FULLY HOMOMORPHIC ENCRYPTION SCHEMES TO SECURE CLOUD COMPUTING

S.S. Skapcov, M.A. Kisel

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The article investigates the issues of ensuring confidentiality during data processing in cloud environments using fully homomorphic encryption technology. This method allows performing mathematical operations on encrypted data without decryption on the server side. An analysis of modern BFV and CKKS schemes is carried out, mechanisms of noise accumulation in ciphertexts are considered, and a model of secure interaction that minimizes the risks of information leakage at the computation stage is proposed.

Keywords: cryptography, homomorphic encryption, cloud computing, data privacy, information security, ciphertext, CKKS scheme, computational complexity, information protection, algorithm.

Введение

Массовый переход к облачным вычислениям создает критическую уязвимость. Традиционные методы шифрования требуют расшифрования данных в оперативной памяти сервера для проведения операций. Это открывает доступ к конфиденциальной информации администраторам провайдера или вредоносному ПО. Полностью гомоморфное шифрование решает эту проблему, позволяя оперировать зашифрованными значениями. Актуальность темы обусловлена необходимостью внедрения концепции

«нулевого доверия» при обработке персональных и финансовых данных в распределенных сетях.

Основная часть

Математическая суть гомоморфного шифрования заключается в существовании гомоморфизма между кольцом открытых текстов и кольцом шифротекстов. Это означает, что результат операции над криптограммами после расшифрования будет идентичен результату аналогичной операции над исходными данными [3].

Современные эффективные схемы, таких как: BFV, CKKS, базируются на задаче обучения с ошибками в кольцах, что делает их устойчивыми к атакам квантовых компьютеров. При зашифровании в структуру данных вносится небольшой случайный параметр - «шум», обеспечивающий стойкость. Однако каждое гомоморфное умножение увеличивает уровень этого шума. При достижении критического порога корректное расшифрование становится невозможным, что требует применения процедуры "bootstrapping" (очистки шума), значительно замедляющей вычисления [1].

Для выбора оптимального решения при проектировании защищенных систем необходимо учитывать особенности различных криптографических схем. Основные характеристики наиболее востребованных алгоритмов представлены в таблице.

Сравнительный анализ схем гомоморфного шифрования
Comparative analysis of homomorphic encryption schemes

Схема	Тип данных	Особенности применения
BFV	Целые числа (Z)	Высокая точность, подходит для баз данных
BGV	Целые числа (Z)	Эффективна для глубоких вычислений (цепей)
CKKS	Числа с плавающей запятой (R/C)	Подходит для статистического анализа и машинного обучения, работает с приближенными значениями
TFHE	Логические значения (биты / Булевы цепи)	Самая быстрая процедура очистки шума (bootstrapping), идеальна для построения произвольной логики

В работе выделены два ключевых направления:

1. Схема BFV – ориентирована на точные вычисления с целыми числами, что необходимо для баз данных и финансового сектора.
2. Схема CKKS – поддерживает арифметику чисел с плавающей запятой. Она допускает контролируемую погрешность, что делает ее оптимальной для нейронных сетей и статистического анализа [2].

Защищенный цикл обработки включает генерацию ключей на стороне клиента, передачу шифротекстов в облако, выполнение сервером «слепых»

операций и возврат зашифрованного результата владельцу. Основным барьером остается вычислительная сложность, однако использование пакетной обработки данных (SIMD) и специализированных библиотек (Microsoft SEAL, OpenFHE) позволяет сократить временные затраты до приемлемых уровней в задачах Big Data

Заключение

Гомоморфная криптография – это фундамент частных вычислений будущего. Несмотря на высокие требования к ресурсам, оптимизация алгоритмов и развитие аппаратных ускорителей делают практическое применение FHE реальным уже сегодня для медицины и финтех. Дальнейшее развитие технологии позволит полностью устранить риск утечки данных на этапе их активной обработки.

Список использованных источников

1. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. - Санкт-Петербург : БХВ-Петербург, 2009. - 576 с.
2. Гентри, К. Полностью гомоморфное шифрование / К. Гентри // СТТ. - 2010. - № 3. - С. 50-55.
3. Мао, В. Современная криптография: теория и практика / В. Мао. - Москва : Вильямс, 2005. - 768 с.

References

1. Panasenko, S. P. Encryption Algorithms. Special Reference Book / S. P. Panasenko. - St. Petersburg: BHV-Petersburg, 2009. - 576 p.
2. Gentry, K. Fully Homomorphic Encryption / K. Gentry // STT. - 2010. - No. 3. - Pp. 50-55.
3. Mao, V. Modern Cryptography: Theory and Practice / V. Mao. - Moscow: Williams, 2005. - 768 p.

Сведения об авторах

Скапцов С.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Кисель М.А., курсанты курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Skapcov S.S., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics"

Kisel M.A., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics"

UDC 004.056:336.71(076)

ENHANCING PERSONAL DATA DE-IDENTIFICATION USING DES-BASED TRANSFORMATION TECHNIQUES

C. Li

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. Operational data sharing often requires stable record linkage while reducing identity disclosure risk. This paper outlines a compact two-layer de-identification design: DES-family deterministic pseudonymization (preferably Triple-DES) to transform direct identifiers into reversible tokens, and k-anonymity-guided generalization/suppression to limit linkage via quasi-identifiers. We show how DES-style permutations can be adapted to format-constrained fields through rank-then-encipher methods, and we summarize key security and utility trade-offs.

Keywords: de-identification; pseudonymization; tokenization; DES; Triple-DES; format-preserving encryption; rank-then-encipher; k-anonymity; quasi-identifiers; re-identification risk.

Introduction

De-identification aims to reduce the chance that released data can be linked back to individuals, while keeping data useful for analysis and operations. In practice, removing names is insufficient because combinations of quasi-identifiers (e.g., date of birth, region, sex) can enable linkage to external datasets, motivating formal models such as k-anonymity [4,5]. At the same time, many workflows require consistent linkage across tables and time; therefore, deterministic, keyed transformations (pseudonymization) are commonly used to replace direct identifiers with stable tokens [5,6].

This paper focuses on DES-based transformation because DES is a well-studied block cipher whose security debate highlights the importance of key length and brute-force feasibility [1,2]. Given modern threats, single-DES (56-bit) should not be relied on; where legacy constraints exist, Triple-DES is the preferred DES-family option for token generation [1,2,3].

Transformation of Personal Data for Anonymization

We propose a two-layer pipeline that separates (A) protection of direct identifiers from (B) control of quasi-identifier linkage risk. Layer A creates reversible pseudonyms (tokens) for identifiers such as account numbers or patient IDs; Layer B generalizes or suppresses quasi-identifiers until the released dataset satisfies a k-anonymity threshold [4,5].

A block cipher is a keyed permutation over fixed-size blocks; under a secret key it maps each input to a unique output and supports inversion with

the same key. DES was standardized for interoperability and scrutinized widely; its 56-bit key length makes exhaustive search increasingly feasible, as early analyses argued [1,2].

For de-identification, we use the permutation property to create deterministic tokens: pack an identifier into one or more 64-bit blocks, apply Triple-DES as the core permutation, and re-encode the result into the field's allowed character set. Determinism preserves referential integrity for joins, while access to keys can be restricted for controlled re-identification [1,3,6].

Many real identifiers have constrained formats (e.g., fixed-length digits). Format-preserving techniques address this by using Rank-then-Encipher (RtE): ranking maps a formatted value to an integer, a block-cipher-based permutation encrypts the integer, and unranking maps it back to the original format [7,8]. RtE aims to preserve only format properties; preserving extra message-specific characteristics can leak information and weaken protection [7].

In a DES-family setting, Triple-DES can serve as the underlying permutation inside RtE when system constraints require it, but designers should apply domain separation (per-field keys or context tweaks) to prevent cross-dataset linkability, especially for small domains where enumeration is practical [8].

k-Anonymity requires that each quasi-identifier pattern in the released dataset correspond to at least k records, reducing the chance that a record uniquely matches an external reference [4]. A practical enforcement method is to iteratively generalize (e.g., date→year, ZIP→region) and suppress outliers until the minimum equivalence-class size reaches k . Empirical work on health datasets shows that algorithm choice affects information loss and runtime, and that optimized methods can improve utility compared to simpler heuristics [6].

Security: deterministic tokens enable linkage, but they remain vulnerable if the token domain is small or if the underlying cipher key is weak; therefore single-DES is unsuitable and Triple-DES should be used when DES is unavoidable [1,2]. Utility: stronger generalization for k -anonymity reduces re-identification risk but degrades analytic precision; selecting k and hierarchies should be guided by intended use and acceptable risk thresholds [5, 6].

Conclusion

A practical way to enhance de-identification is to combine cryptographic pseudonymization of direct identifiers with formal control of quasi-identifier linkage. DES-family permutations (preferably Triple-DES) can generate stable, reversible tokens and can be adapted to format-constrained fields via RtE methods. k -Anonymity then reduces linkage risk by ensuring non-unique quasi-identifier patterns, with an explicit privacy–utility trade-off

References

1. Smid, M. E., & Branstad, D. K. (2002). Data encryption standard: past and future. *Proceedings of the IEEE*, 76(5), 550-559.
2. Diffie, W., & Hellman, M. E. (2006). Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, 10(6), 74-84.
3. Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & sons.
4. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, 10(05), 557-570.
5. El Emam, K. (2011). Methods for the de-identification of electronic health records for genomic research. *Genome medicine*, 3(4), 25.
6. El Emam, K., Dankar, F. K., Issa, R., Jonker, E., Amyot, D., Cogo, E., ... & Bottomley, J. (2009). A globally optimal k-anonymity method for the de-identification of health data. *Journal of the American Medical Informatics Association*, 16(5), 670-682.
7. Weiss, M., Rozenberg, B., & Barham, M. (2015). Practical solutions for format-preserving encryption. *arXiv preprint arXiv:1506.04113*.
8. Durak F. B., Horst H., Horst M., Vaudenay S. (2021) FAST: Secure and High Performance Format-Preserving Encryption and Tokenization. In: ASIACRYPT 2021, LNCS 13092, 465–489. Springer.

Information about the authors

Li. C., Master's Student of Engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lcaomi@outlook.com.

УДК 004.056.55

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИСТОЧНИКОВ ИЗЛУЧЕНИЯ ДЛЯ ШИФРОВАНИЯ С ПОМОЩЬЮ КВАНТОВЫХ ТОЧЕК

А.Ю. Ефремова, В.М. Алефиренко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье сравниваются источники излучения, используемые при шифровании информации на основе спектров поглощения квантовых точек. Проанализированы этапы проведения процедуры шифрования, а также технические средства, необходимые для этого. Особое внимание уделено правильности выбора источников излучения. В результате сравнительного анализа источников излучения выявлено, что оптимальный выбор источника повышает точность, воспроизводимость и устойчивость криптографической системы.

Ключевые слова: защита информации, шифрование, криптография, квантовые технологии, квантовые точки, спектр, источник излучения, ультрафиолетовое (УФ) излучение, инфракрасное (ИК) излучение.

COMPARATIVE ANALYSIS OF RADIATION SOURCES USED FOR ENCRYPTION BASED ON QUANTUM DOTS

A.Y. Yafremava, V.M. Alefirenko

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article compares radiation sources used in information encryption based on the absorption spectra of quantum dots. The stages of the encryption procedure, as well as the technical means required for its implementation, are analyzed. Particular attention is paid to the correct selection of radiation sources. As a result of the comparative analysis, it was found that the optimal choice of source improves the accuracy, reproducibility, and robustness of the cryptographic system.

Keywords: information security, encryption, cryptography, quantum technologies, quantum dots, spectrum, radiation source, ultraviolet (UV) radiation, infrared (IR) radiation.

Введение

В связи с непрекращающимся развитием квантовых технологий в области защиты информации, крайне важно уделить внимание исследованиям в области квантовой криптографии.

Особый интерес представляет шифрование с использованием квантовых точек – наноразмерных полупроводниковых структур, обладающих дискретным спектром энергетических уровней и оптическими характеристиками, которые позволяют формировать уникальные спектральные сигнатуры, применимые в задачах шифрования и аутентификации [1].

Основная часть

Идея шифрования информации на основе спектров поглощения квантовых точек заключается в использовании многомерного спектрального отклика как физического носителя шифра: либо как физического ключа, либо как носителя многоканального спектрального шифрования.

Для дальнейшего сравнения технических средств, необходимо для начала рассмотреть этапы проведения процедуры шифрования: подготовка образца; калибровка; измерение спектра; проверка повторяемости; проверка аддитивности и линейности; формирование криптографического ключа; дешифрование и оценка ошибок.

Чтобы такой подход был воспроизводим, требуется целый технологический комплекс, состоящий из источников излучения, спектрометров/монокроматоры, вещества-детекторы, оптическая обвязка в виде фильтров, держателей, интегрирующих сфер, генераторов, а при необходимости – криогенных систем (криостаты) и микроскопию.

Выбор источника излучения является критически важным фактором при реализации схем шифрования на основе спектров поглощения квантовых точек, поскольку именно он определяет характер формируемого спектрального отклика, его стабильность и воспроизводимость [2,3].

В связи с этим далее в таблице будет представлено сравнение нескольких источников излучения.

Сравнительный анализ источников излучения, используемых для шифрования с помощью КТ
KT Comparative analysis of radiation sources used for encryption based on quantum dots

Характеристика	Дейтериевая лампа	Вольфрам-галогенная лампа	Ксеноновая лампа	LED / лазер
Спектральная полезность	Используется для УФ-области	Используется в видимой и ближней ИК-области	Широкополосный и интенсивный источник	Узкополосное излучение, используется только для отдельных каналов
Интенсивность сигнала	Не универсален для всего диапазона	Используется только для Vis/NIR	Одна из лучших по интенсивности	Используется только для выбранной длины волны
Воспроизводимость измерений	Используется только при стабильном режиме работы	Используется для рутинных измерений	Используется только в сочетании с качественной оптикой	Используется только для фиксированного канала
Гибкость для разных КТ	Используется при критичной УФ-область	Используется при видимых рабочих диапазонах	Используется для разных составов КТ и задач	Используется только для частных схем
Пригодность для криптосистемы	Используется в комбинированных системах	Используется в комбинированных системах	Используется для полноценного спектрального шифрования	Используется для упрощенных систем
Лучший сценарий шифрования	Точный анализ УФ-полос	Базовые Vis/NIR измерения	Полноспектральная исследовательская установка	Дешевый компактный прототип

Заключение

В ходе сравнения установлено, что для построения надежных систем шифрования на основе квантовых точек наибольшую ценность представляют широкополосные и интенсивные источники излучения, способные обеспечить одновременное возбуждение и регистрацию широкого диапазона длин волн, однако комбинирование различных типов

источников может рассматриваться как наиболее перспективный подход, позволяющий объединить преимущества широкополосных и узкополосных систем.

Список использованных источников

1. Ефремова, А. Ю., Алефиренко В.М. (2025) Комплексное сравнение качественных показателей надежности при моделировании системы шифрования с использованием квантовых точек. *Современные средства связи : материалы XXX Международной научно-технической конференции*. 100–102.
2. Meng H., Gao Y., Wang X., Li X., Wang L., Zhao X., et al. (2024) Quantum dot-enabled infrared hyperspectral imaging with single-pixel detection. *Light: Science & Applications*. 13 (121).
3. Jiang M., Li X., Wang J., Wen Y. (2025). Research on the impact of blood absorption on the photothermal effect of nanoparticles with protein corona. *Physical Chemistry Chemical Physics*. 27, 25087–25097.

References

1. Yafremava, A. Yu., Alefirenko, V. M. (2025). Comprehensive comparison of qualitative reliability indicators in modeling an encryption system based on quantum dots. *Modern Communication Means: Proceedings of the XXX International Scientific and Technical Conference*, 100–102 (in Russian).
2. Meng H., Gao Y., Wang X., Li X., Wang L., Zhao X., et al. (2024) Quantum dot-enabled infrared hyperspectral imaging with single-pixel detection. *Light: Science & Applications*. 13 (121).
3. Jiang M., Li X., Wang J., Wen Y. (2025). Research on the impact of blood absorption on the photothermal effect of nanoparticles with protein corona. *Physical Chemistry Chemical Physics*. 27, 25087–25097. 2.

Сведения об авторах

Ефремова А.Ю., ассистент каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.

Алефиренко В.М., кандидат технических наук, доцент, доцент каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alefirenko@bsuir.by.

Information about the authors

Yafremava A.Yu., Assistant of the department Information and Computer-Aided Systems Design, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, al617e13@gmail.com.

Alefirenko V.M., Cand. Sci. (Tech.), Associate professor of the department Information and Computer-Aided Systems Design. Educational Institution “Belarusian State University of Informatics and Radioelectronics”, alefirenko@bsuir.by.

УДК 004.056.55 / 543.42.061

СРАВНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ СПЕКТРАЛЬНОГО АНАЛИЗА, ИСПОЛЪЗУЕМЫХ В КВАНТОВОЙ КРИПТОГРАФИИ

А.Ю. Ефремова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье приведено сравнение технических средств спектрального анализа, используемых в квантовой криптографии. Приводится описание использования спектроскопии в сфере шифрования информации. Рассматриваются перспективы перехода к более высокому уровню защищенности данных. Особое внимание уделено правильности выбора технических средств спектрального анализа. По результатам сравнения выявлено, что выбор технического средства влияет на точность, устойчивость и практическую реализуемость систем шифрования информации.

Ключевые слова: защита информации, криптография, шифрование, квантовые технологии, спектральный анализ, технические средства, оптический фильтр, монохроматор, спектрометр.

COMPARISON OF SPECTRAL ANALYSIS INSTRUMENTS USED IN QUANTUM CRYPTOGRAPHY

A.Yu. Yafremava

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article presents a comparison of spectral analysis instruments used in quantum cryptography. It describes the use of spectroscopy in the field of information encryption and considers the prospects for achieving a higher level of data security. Particular attention is paid to the correct selection of spectral analysis instruments. Based on the comparison, it was found that the choice of technical instrument affects the accuracy, robustness, and practical feasibility of information encryption systems.

Keywords: information protection, cryptography, encryption, quantum technologies, spectral analysis, technical instruments, optical filter, monochromator, spectrometer.

Введение

В условиях стремительного роста вычислительных возможностей квантовых компьютеров, особую актуальность приобретает поиск новых подходов к защите информации, способных обеспечить высокий уровень устойчивости к атакам. Эти обстоятельства способствовали росту интереса к различным методам квантовой криптографии, в том числе и к комплексным подходам, в которых защита информации обеспечивается не только алгоритмическими преобразованиями, но и за счет уникальных физических характеристик оптического сигнала, материала и излучения [1,2].

Основная часть

Отдельный интерес представляют системы, сочетающие методы защиты информации со средствами спектрального анализа. Поскольку спектроскопия позволяет использовать спектральные, временные и поляризационные характеристики оптических сигналов в качестве дополнительных носителей информации, такой подход делает возможным реализацию новых схем шифрования, аутентификации и скрытой передачи данных. Однако стоит отметить, что такие системы отличаются высокой сложностью как с точки зрения структуры, так и с точки зрения практической реализации, что делает особенно важным корректный выбор технических средств, применяемых для формирования, регистрации и анализа спектральных характеристик.

В связи с этим далее проводится сравнение технических средств, используемых в качестве элементов спектрального анализа в системах шифрования информации [2–4].

Сравнение технических средств спектрального анализа, используемых в квантовой криптографии

Comparison of spectral analysis instruments used in quantum cryptography

Тип технического средства	Набор оптических фильтров	Одинарный монохроматор	Двойной монохроматор	Спектрометр с многоканальным массивом
1	2	3	4	5
Спектральная избирательность	Низкая	Средняя	Высокая	Средняя/высокая в зависимости от прибора и решетки
Подавление паразитного света	Низкое	Среднее	Высокое	Среднее/высокое в зависимости от конструкции
Гибкость по длинам волн	Низкая	Высокая	Очень высокая	Высокая в пределах рабочего окна
Скорость получения данных	Высокая для фиксированн ых каналов	Низкая/ средняя	Низкая, из-за усложнения тракта	Высокая
Пригодность для сложных шифровальных схем	Ограниченная	Хорошая	Очень хорошая	Очень хорошая
Пригодность для точного сравнения близких спектров КТ	Не подходящая	Подходящая	Наиболее подходящая	Подходящая, особенно при необходимости быстрого захвата спектра

Продолжение таблицы
Continuation of table

1	2	3	4	5
Сложность реализации	Низкая	Средняя	Высокая	Средняя/высокая
Лучший Сценарий использования	Дешевый прототип	Базовая лабораторная установка	Максимальная точность и подавление шумов	Практичная система с высокой скоростью

Заключение

Сравнение показывает, что выбор технических средств спектрального анализа напрямую влияет на точность, устойчивость и практическую реализуемость систем шифрования информации. Наборы оптических фильтров, являясь доступным решением, подходят для простых и демонстрационных схем и не эффективны при работе со сложными многоканальными методами. Монохроматоры обеспечивают более высокую точность и универсальность, что делает их подходящими для лабораторных исследований. В то же время спектрометры с многоканальным массивом представляют собой наиболее практичный компромисс между скоростью, гибкостью и качеством регистрации, что делает их особенно перспективными для построения прикладных и высокоскоростных систем спектрального шифрования.

Из всего вышеперечисленного следует, что выбор конкретного прибора должен определяться целями системы, требованиями к точности измерений, скорости обработки данных и условиям практического применения.

Список использованных источников

1. Ефремова, А. Ю., Морозова А.Н. (2025) Сравнительный анализ классических и квантовых методов шифрования. *Технические средства защиты информации: материалы XXIII Международной научно-технической конференции*. 154–157.
2. Mamann H., Nieddu T., Hoffet F., Bozzio M., Garreau de Loubresse F., Kerenidis I., Dia-manti E., Urvoy A., Laurat J. (2025) Quantum cryptography integrating an optical quantum memory. *Science Advances*. 11 (38).
3. Tan H., Petrov M., Zhang W., Han L., Liao S.-K., Makarov V., Xu F., Pan J.-W. (2025) Wide-Spectrum Security of Quantum Key Distribution. *PRX Quantum*. 2025.(6).
4. Tunsiri S., Kanthavong S., Louangvilay, Mitatha S., Yupapin P. P. (2012) Optical-Quantum Security using Dark-Bright Soliton Conversion in a Ring Resonator System. *Procedia Engineering*. (32), 475–481.

References

1. Yafremava, A. Yu., Morozova, A. N. (2025). Comparative Analysis of Classical and Quantum Encryption Methods. Technical Means of Information Protection: Proceedings of the 23rd International Scientific and Technical Conference, 154–157 (in Russian).
2. Mamann H., Nieddu T., Hoffet F., Bozzio M., Garreau de Loubresse F., Kerenidis I., Dia-manti E., Urvoy A., Laurat J. (2025) Quantum cryptography integrating an optical quantum memory. Science Advances. 11 (38).
3. Tan H., Petrov M., Zhang W., Han L., Liao S.-K., Makarov V., Xu F., Pan J.-W. (2025) Wide-Spectrum Security of Quantum Key Distribution. PRX Quantum. 2025.(6).
4. Tunsiri S., Kanthavong S., Louangvilay, Mitatha S., Yupapin P. P. (2012) Optical-Quantum Security using Dark-Bright Soliton Conversion in a Ring Resonator System. Procedia Engineering. (32), 475–481.

Сведения об авторах

Ефремова А.Ю., ассистент каф. проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.

Information about the authors

Yafremava, A. Yu., Assistant of the department Information and Computer-Aided Systems Design, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, al617e13@gmail.com.

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ ПОДХОДОВ К АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В.А. Герасимов

*Научно-исследовательский институт технической защиты информации,
г. Минск, Республика Беларусь*

Аннотация. Проведен теоретический анализ безопасности трех подходов к аутентификации пользователя в Hardware Security Module (HSM) для систем электронной цифровой подписи на основе виртуальной инфраструктуры: 1) централизованный контроль на основе данных активации подписи (авторский подход); 2) разделение ключа с кворумом M-of-N; 3) разделение ключа с хранением части на стороне пользователя. Проведен анализ соответствия перечисленных подходов стандарту PKCS#11, определяющему унифицированный интерфейс взаимодействия с HSM. Предложены модели для расчета вероятностей успешной атаки для этих подходов. Обосновано, что авторский подход обеспечивает оптимальный баланс между безопасностью и сложностью реализации.

Ключевые слова: электронная цифровая подпись; виртуальная инфраструктура; HSM; аутентификация; данные активации подписи; PKCS#11.

COMPARATIVE ANALYSIS OF SECURITY OF USER AUTHENTICATION APPROACHES IN ELECTRONIC DIGITAL SIGNATURE SYSTEMS BASED ON VIRTUAL INFRASTRUCTURE

V.A. Gerasimov

*Research Institute for Technical Protection of Information,
Minsk, Republic of Belarus*

Abstract. A theoretical security analysis of three approaches to user authentication in the Hardware Security Module (HSM) for electronic digital signature systems based on a virtual infrastructure is performed: 1) centralized control based on signature activation data (the author's approach); 2) key sharing with M-of-N quorum; 3) key sharing with storage of a part on the user side. An analysis of the compliance of the listed approaches with the PKCS#11 standard, which defines a unified interface for interaction with the HSM, is carried out. Models for calculating the probabilities of a successful attack for these approaches are proposed. It is substantiated that the author's approach provides an optimal balance between security and implementation complexity.

Keywords: electronic digital signature; virtual infrastructure; HSM; authentication; signature activation data; PKCS#11.

Введение

Обеспечение безопасности личного ключа является критической задачей при выработке электронной цифровой подписи (ЭЦП). Использование HSM, т. е. аппаратных модулей безопасности, позволяет минимизировать риски компрометации, однако вопрос надежной аутентификации пользователя перед HSM остается предметом научных дискуссий [1, 2]. Стандарт PKCS#11 определяет платформонезависимый программный интерфейс для взаимодействия с криптографическими устройствами [5]. Этот стандарт поддерживается большинством современных HSM и криптографических токенов, что делает его важным критерием при оценке практической применимости рассматриваемых подходов. Существующие решения можно классифицировать на три категории: централизованные протоколы с активацией подписи, схемы разделения ключа с пороговым доступом (кворум) и схемы с распределенным хранением ключа между HSM и клиентом. Целью данной работы является сравнительный анализ указанных подходов с точки зрения безопасности, соответствия стандарту PKCS#11 и практической реализуемости.

Основная часть

В рамках исследования были рассмотрены три подхода аутентификации и доступа к ключу в HSM для создания ЭЦП в системах на основе виртуальной инфраструктуры.

Подход 1. Протокол активации подписи с использованием ДАП (авторский). Пользователь хэширует документ и аутентифицируется, генерируя уникальные данные активации подписи (ДАП). Хэш документа через сервер подписи и ДАП (по защищенному каналу) поступают в HSM, который после проверки ДАП вырабатывает подпись ключом пользователя. Важной особенностью является то, что вызов криптографических функций HSM осуществляется от имени СП, но только при наличии валидных ДАП.

Подход 2. Разделение ключа по схеме M-of-N. Личный ключ K разделяется на N частей (например, 5) с использованием алгоритма разделения секрета Шамира [3] и распределяется по независимым HSM. Для сборки ключа и подписания необходимо получить и объединить M частей (например, 3) от разных модулей.

Подход 3. Разделение ключа на две части (HSM и клиент). Ключ K разделен на две компоненты: K_{HSM} , хранящуюся в HSM, и K_{client} , хранящуюся в защищенной области на устройстве пользователя. Подпись генерируется путем объединения результатов вычислений от обеих частей.

Результаты сравнительного анализа подходов с учетом вероятностных моделей и соответствия стандарту PKCS#11.

Результаты сравнительного анализа подходов
Results of the approaches comparative analysis

Параметр / Угроза	Подход 1	Подход 2	Подход 3
1	2	3	4
Вероятность компрометации и ключа	$p \cdot q (\sim 10^{-9})$	$\sum_{k=M}^N C_N^k p^k (1-p)^{N-k} (\sim 10^{-8})$	$p \cdot p_c (\sim 10^{-5})$
Соответствие PKCS#11	Полное (стандартная функция C_Sign с атрибутом SCA_ALWAYS_AUTHENTICATE; вызов от имени СП)	Частичное (требуется проприетарные расширения)	Частичное (требуется экспортируемый ключ, SCA_EXTRACTABLE = true)
Стойкость к сговору	Высокая (требуется участие пользователя)	Низкая (возможен сговор М операторов)	Средняя
Зависимость от безопасности клиента	Низкая (клиент только генерирует ДАП)	Очень низкая (ключ не хранится у клиента)	Высокая (часть ключа – у клиента)
Сложность реализации	Низкая	Высокая (синхронизация, управление долями)	Средняя

Заключение

1. Авторский подход может быть реализован с использованием стандартных механизмов (C_Sign с атрибутом SKA_ALWAYS_AUTHENTICATE) [2; 5]. Важной особенностью является то, что вызов криптографических функций осуществляется от имени сервера подписи, но только при наличии валидных ДАП, что гарантируется аппаратными механизмами HSM. Распределенный подход M-of-N требует проприетарных расширений API [3], а подход с разделением ключа – установки атрибута SKA_EXTRACTABLE, что снижает безопасность [5].

2. Авторский подход превосходит по теоретической стойкости подход с кворумом M-of-N при типичных значениях вероятностей компрометации.

3. Подход с разделением ключа на две части демонстрирует критическую зависимость от безопасности клиентской среды, что делает его наименее предпочтительным для систем с высокими требованиями к защите.

4. Авторский подход демонстрирует наилучший баланс между количественными показателями безопасности, соответствием отраслевым стандартам и сложностью реализации, что делает его предпочтительным для внедрения в системах электронной цифровой подписи на основе виртуальной инфраструктуры [1, 2, 4].

Список использованных источников

1. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов, М. А. Казловский, О. В. Бойправ // Комплексная защита информации: материалы XXVIII науч.-практ. конф. — Гомель: БелГУТ, 2023. — С. 257–261.
2. Герасимов, В. А. Использование системы облачной электронной подписи для организации электронного голосования / В. А. Герасимов, М. А. Казловский // Цифровая трансформация. — 2024. — Т. 30, № 1. — С. 52–62.
3. Шамир, А. Как разделить секрет / А. Шамир // Коммуникации АСМ. — 1979. — Т. 22, № 11. — С. 612–613.
4. Герасимов, В. А. Метод обнаружения событий информационной безопасности в системах облачной подписи / В. А. Герасимов, О. В. Бойправ // Цифровая трансформация. — 2024. — Т. 30, № 2. — С. 77–84.
5. RSA Laboratories. PKCS #11 v2.40: Cryptographic Token Interface Standard. — 2015. — 422 с.

References

1. Herasimau V. A., Kazlouski M. A., Boiprav O. V. (2023) Information protection mechanisms in the development of cloud-based electronic digital signatures. *Integrated*

Information Protection: Proceedings of the XXVIII Scientific and Practical Conference. Gomel, BelSUT, pp. 257–261. (In Russian)

2. Herasimau V. A., Kazlouski M. A. (2024) Using a Cloud-Based Electronic Signature System for Organizing Electronic Voting. *Digital Transformation*. 30 (1), 52–62. (In Russian)

3. Shamir A. (1979) How to share a secret. *Communications of the ACM*. 22 (11), 612–613.

4. Gerasimov V. A., Boyprav O. V. (2024) Method for Information Security Events Detection in a Cloud Signature Systems. *Digital Transformation*. 30 (2), 77–84. (In Russian)

5. RSA Laboratories. (2015) PKCS #11 v2.40: Cryptographic Token Interface Standard.

Сведения об авторе

Герасимов В. А., магистр, сотрудник Научно-исследовательского института технической защиты информации, e-mail: vger@niitzi.by.

Information about the author

Gerasimov V., Master of Science, Researcher at the Research Institute for Technical Protection of Information, e-mail: vger@niitzi.by.

УДК 004.056

ПРИМЕНЕНИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВЫХ СИСТЕМАХ

М.М. Ходжамаммедов

*Государственный энергетический институт Туркменистана, г.
Мары, Туркменистан*

Аннотация. В статье представлен комплексный научный анализ применения постквантовой криптографии как ключевого направления обеспечения информационной безопасности в условиях развития квантовых вычислений. Рассматриваются ограничения классических криптографических методов, обусловленные появлением квантовых алгоритмов, а также исследуются современные подходы к построению устойчивых криптосистем. Особое внимание уделено решеточным, кодовым и хэш-ориентированным алгоритмам, а также вопросам их практической интеграции в цифровые инфраструктуры. Обоснована необходимость перехода к криптографическим решениям нового поколения.

Ключевые слова: постквантовая криптография; квантовые вычисления; защита информации; криптографическая устойчивость; цифровая безопасность; алгоритмы; киберугрозы.

APPLICATION OF POST-QUANTUM CRYPTOGRAPHY FOR INFORMATION SECURITY IN DIGITAL SYSTEMS

M.M. Hojamammedow

State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The paper presents a comprehensive scientific analysis of post-quantum cryptography as a key approach to ensuring information security in the context of quantum

computing development. The limitations of classical cryptographic methods caused by quantum algorithms are examined, and modern approaches to building quantum-resistant cryptosystems are analyzed. Particular attention is paid to lattice-based, code-based, and hash-based methods, as well as their practical integration into digital infrastructures. The necessity of transitioning to next-generation cryptographic solutions is substantiated.

Keywords: post-quantum cryptography; quantum computing; information security; cryptographic strength; digital security; algorithms; cyber threats.

Введение

Стремительное развитие цифровых технологий и переход к новым вычислительным парадигмам формируют качественно новые вызовы в области информационной безопасности. Одним из наиболее значимых факторов является развитие квантовых вычислений, способных радикально изменить существующие подходы к защите информации. В этих условиях традиционные криптографические алгоритмы постепенно утрачивают свою надежность, что обуславливает необходимость поиска альтернативных решений.

Появление квантовых алгоритмов, ориентированных на решение сложных математических задач, лежащих в основе современных криптосистем, создает предпосылки для их потенциальной компрометации. Это делает актуальным переход к новым криптографическим механизмам, способным обеспечить устойчивость к принципиально иным типам вычислительных атак.

Основная часть

Постквантовая криптография представляет собой перспективное направление, ориентированное на разработку алгоритмов, устойчивых к воздействию как классических, так и квантовых вычислительных средств. В отличие от традиционных методов, ее основой являются математические задачи, сохраняющие вычислительную сложность даже при использовании квантовых технологий.

Одним из наиболее активно развивающихся направлений является решетчатая криптография. Данный подход базируется на сложных задачах многомерной геометрии, решение которых остается вычислительно трудоемким. Практическая значимость таких алгоритмов определяется их высокой производительностью и возможностью применения в различных криптографических протоколах.

Кодовые криптосистемы представляют собой еще одно важное направление. Их устойчивость основана на сложности декодирования случайных линейных кодов. Несмотря на значительные требования к объему ключевой информации, такие системы демонстрируют высокий уровень надежности и активно рассматриваются как кандидаты для стандартизации.

Хэш-ориентированные методы обеспечивают безопасность за счет использования криптографических хэш-функций. Они находят широкое применение в системах цифровой подписи и отличаются высокой степенью формальной обоснованности безопасности.

Современные исследования в области постквантовой криптографии направлены не только на разработку новых алгоритмов, но и на их адаптацию к существующим цифровым системам. Важным аспектом является обеспечение совместимости с действующими протоколами и инфраструктурой, что требует создания гибридных решений, сочетающих классические и постквантовые методы защиты.

Отдельного внимания заслуживает процесс международной стандартизации постквантовых алгоритмов. Ведущие научные организации активно проводят исследования и отбор наиболее перспективных решений, что подтверждает стратегическую значимость данного направления для глобальной информационной безопасности.

Заключение

Таким образом, постквантовая криптография является ключевым элементом формирования устойчивых систем защиты информации в условиях цифровой трансформации. Переход к новым криптографическим стандартам представляет собой необходимый этап эволюции информационной безопасности. Дальнейшее развитие данной области связано с совершенствованием алгоритмов, оптимизацией их реализации и интеграцией в современные цифровые инфраструктуры.

Список использованных источников

1. NIST. Post-Quantum Cryptography Standardization. 2023.
2. Bernstein D. Lattice-Based Cryptography. 2021.
3. Alagic G. Status Report on PQC. 2024.
4. Chen L. Post-Quantum Cryptography Report. 2022.

References

1. NIST. Post-Quantum Cryptography Standardization, 2023.
2. Bernstein D. Lattice-Based Cryptography, 2021.
3. Alagic G. PQC Status Report, 2024.
4. Chen L. Post-Quantum Cryptography Report, 2022.

Сведения об авторе

Ходжамаммедов М.М. – преподаватель кафедры информационных технологий, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com.

Information about the author

Hojamammedow M.M. – Lecturer of the Department of Information Technologies, State Energy Institute of Turkmenistan, Mary, Turkmenistan, mekanhoja2021@gmail.com.

УДК 004.056

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И РОСТА КИБЕРУГРОЗ

М.М. Ходжамаммедов, Ю.Т. Джумагылджов, М.М. Мухаммедов

*Государственный энергетический институт Туркменистана,
г. Мары, Туркменистан*

Аннотация. В статье исследуются современные научно-технические подходы к обеспечению технической защиты информации в условиях цифровой трансформации и экспоненциального роста киберугроз. Проведен системный анализ каналов утечки информации, включая побочные электромагнитные излучения и наводки, физический доступ и уязвимости инфраструктуры. Рассмотрены методы повышения защищенности информационных систем на основе интеграции интеллектуальных технологий мониторинга, предиктивной аналитики и адаптивных систем безопасности. Обоснована необходимость комплексного подхода к защите информации на всех уровнях ее обработки и передачи.

Ключевые слова: техническая защита информации; кибербезопасность; побочные каналы утечки; электромагнитная совместимость; интеллектуальные системы; цифровая безопасность; мониторинг.

TECHNICAL INFORMATION SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION AND CYBER THREATS

M.M. Hojamammedow, Y.T. Jumaglyjov, M.M. Muhammedov

State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The paper investigates modern scientific and technical approaches to ensuring technical information security in the context of digital transformation and rapidly increasing cyber threats. A systematic analysis of information leakage channels, including electromagnetic emanations, physical access, and infrastructure vulnerabilities, is carried out. Methods for improving information system security based on intelligent monitoring technologies, predictive analytics, and adaptive security systems are considered. The necessity of a comprehensive approach to information protection at all stages of processing and transmission is substantiated.

Keywords: technical information protection; cybersecurity; side-channel leakage; electromagnetic compatibility; intelligent systems; digital security; monitoring.

Введение

Современный этап развития информационного общества характеризуется интенсивной цифровизацией всех сфер деятельности, что сопровождается значительным увеличением объемов обрабатываемой информации и усложнением архитектуры информационных систем. В этих условиях

возрастает актуальность обеспечения технической защиты информации, направленной на предотвращение утечки данных по техническим каналам.

Особую опасность представляют побочные каналы утечки информации, возникающие в результате физических процессов в электронных устройствах. К ним относятся электромагнитные излучения, акустические сигналы, паразитные токи и наводки. Анализ подобных угроз требует междисциплинарного подхода, объединяющего методы радиотехники, электроники и теории информации [1].

Основная часть

Техническая защита информации представляет собой совокупность организационных и инженерно-технических мер, направленных на предотвращение несанкционированного доступа и утечки данных через физические и технические каналы. В рамках данной концепции особое значение приобретает защита от побочных электромагнитных излучений и наводок (ПЭМИН).

Математическая модель вероятности утечки информации через технические каналы может быть описана следующим выражением:

$$P_{\text{ут}} = 1 - e^{-\lambda t}, \quad (1)$$

где λ — интенсивность возникновения угроз, t — время воздействия потенциального канала утечки.

Снижение вероятности утечки достигается за счет применения комплекса технических средств защиты, включающего экранирование, фильтрацию сигналов, заземление и использование специализированных средств подавления излучений. Эффективность экранирования определяется коэффициентом экранирования:

$$K_{\text{э}} = 20 \log \left(\frac{E_1}{E_2} \right) \quad (2)$$

где E_1 и E_2 — уровни электромагнитного поля до и после экранирования соответственно.

В условиях цифровизации значительную роль играют интеллектуальные системы мониторинга, основанные на технологиях искусственного интеллекта и машинного обучения. Такие системы позволяют выявлять аномальные события и прогнозировать возможные атаки на основе анализа больших данных [2].

Дополнительным направлением является внедрение систем контроля и управления доступом (СКУД), а также видеонаблюдения с функциями интеллектуального анализа. Интеграция этих систем в единую платформу безопасности обеспечивает комплексный контроль защищаемых объектов.

Особое внимание уделяется защите информации в распределенных и облачных системах, где увеличивается поверхность атаки. В таких условиях необходима реализация принципов многоуровневой защиты (Defense in Depth), включающей как технические, так и программные средства безопасности.

Заключение

Таким образом, техническая защита информации в условиях цифровой трансформации требует комплексного и научно обоснованного подхода. Применение современных технологий, включая интеллектуальные системы анализа и мониторинга, позволяет существенно повысить уровень защищенности информационных ресурсов. Дальнейшие исследования должны быть направлены на разработку адаптивных систем защиты, способных эффективно противодействовать новым видам угроз.

Список использованных источников

1. Иванов И.И. Методы технической защиты информации. М.: Энергия, 2022.
2. Zhang Y. Artificial Intelligence in Cybersecurity // Energy Reports. 2024. Vol. 10. P. 200–210.
3. Kumar R. Cybersecurity and Smart Systems // Renewable Energy. 2023. Vol. 180. P. 500–510.

References

1. Ivanov I.I. Methods of Technical Information Protection. Moscow, 2022.
2. Zhang Y. Artificial Intelligence in Cybersecurity. Energy Reports, 2024.
3. Kumar R. Cybersecurity and Smart Systems. Renewable Energy, 2023.

Сведения об авторах

Ходжамаммедов М.М. – преподаватель кафедры информационных технологий, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com

Джумагылджов Ю.Т. – студент, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан.

Мухаммедов М.М. – студент, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан.

Information about the authors

Hojamammedow M.M. – Lecturer of the Department of Information Technologies, State Energy Institute of Turkmenistan, Mary, Turkmenistan.

Jumagylyjov Y.T. – Student, State Energy Institute of Turkmenistan, Mary, Turkmenistan.

Muhammedov M.M. – Student, State Energy Institute of Turkmenistan, Mary, Turkmenistan.

УДК 004.056.53

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ КАК ПЕРСПЕКТИВНЫЙ МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Савчук

*Учреждение образования «Гомельский государственный университет
имени Франциска Скорины», г. Гомель, Республика Беларусь*

Аннотация. В статье рассматривается квантовое распределение ключей (QKD) как перспективный метод криптографической защиты информации. Обоснована актуальность применения квантовой криптографии в условиях развития квантовых вычислений, способных снизить устойчивость классических алгоритмов. Описаны принципы работы QKD, включая использование кубитов и протокол BB84. Проанализированы основные преимущества метода, такие как независимость от вычислительных ресурсов и возможность обнаружения перехвата, а также ограничения, связанные с технической реализацией. Сделан вывод о высокой перспективности технологии для обеспечения безопасности передачи данных.

Ключевые слова: квантовая криптография; QKD; информационная безопасность; криптография; квантовые вычисления; протокол BB84; кубиты; защита информации; передача ключей; квантовые технологии

QUANTUM KEY DISTRIBUTION AS A PROMISING METHOD OF CRYPTOGRAPHIC INFORMATION SECURITY

V.V. Savchuk

*Educational Institution “Francisk Skorina Gomel State University, Gomel”,
Republic of Belarus*

Annotation. This article examines quantum key distribution (QKD) as a promising method of cryptographic information security. The relevance of applying quantum cryptography in the context of the development of quantum computing, which can reduce the stability of classical algorithms, is substantiated. The operating principles of QKD are described, including the use of qubits and the BB84 protocol. The main advantages of the method, such as independence from computing resources and the ability to detect interception, are analyzed, as well as the limitations associated with technical implementation. It is concluded that this technology has high potential for ensuring data transmission security.

Keywords: quantum cryptography; QKD; information security; cryptography; quantum computing; BB84 protocol; qubits; information security; key transfer; quantum technologies

Введение

Квантовая криптография – это наука о шифровании данных методами, основанными на законах квантовой механики. В отличие от традиционной криптографии, квантовое шифрование предполагает защиту и передачу данных при помощи физических свойств элементарных частиц [1]. Ключевым направлением квантовой криптографии является квантовое распределение ключей (QKD). Перспективность данного метода

обусловлена использованием квантового состояния частиц, изменение которых при измерении позволяет выявлять вмешательство третьей стороны при передаче информации.

Основная часть

Безопасность метода квантового распределения ключей обусловлена тем, что внешнее воздействие на квантовое состояние приводит к изменению передаваемых данных.

Передача информации осуществляется с использованием кубитов. Кубиты – квантовые аналоги классических битов. В отличие от обычного бита, принимающего значение 0 или 1, кубит может находиться в состоянии суперпозиции, при котором он может принимать значение 1 и 0 одновременно. Наглядный пример – подбрасывание монеты: после падения фиксируется один из двух состояний – «орел» или «решка», но в процессе движения невозможно однозначно определить исход, так как до момента наблюдения он не зафиксирован, можно сказать, что во время полета монета находится в двух состояниях. Принцип суперпозиции кубита позволяет реализовать специальные способы кодирования, используемые в квантовых протоколах.

Наиболее известным протоколом квантового распределения ключей является BB84, предложенный Ч. Беннетом и Ж. Brassаром в 1984 году. В рамках данного протокола передающая сторона кодирует информацию в квантовых состояниях фотонов, используя два различных базиса. Принимающая сторона выполняет измерения, случайным образом выбирая базис измерения для каждого фотона. После передачи участники по открытому каналу обмениваются информацией о выбранных базисах и оставляют только те биты, для которых базисы совпали. Полученная последовательность используется для формирования секретного ключа. Вмешательство третьего лица в процессе передачи приводит к увеличению уровня ошибок в полученных данных. Если количество ошибок превышает допустимое значение, передача признается ненадежной, а сформированный ключ не используется. Таким образом, протокол BB84 позволяет не только передавать ключ, но и контролировать безопасность канала связи [2].

Квантовое распределение ключей обладает рядом принципиальных преимуществ по сравнению с классическими методами криптографической защиты информации.

Во-первых, безопасность QKD не зависит от сложности математических задач, следовательно и от вычислительных возможностей нарушителя. В классической криптографии устойчивость алгоритмов может снижаться с ростом вычислительной мощности, тогда как

в квантовых системах защита основана на физических свойствах квантовых состояний, которые невозможно измерить без их изменения.

Во-вторых, QKD обеспечивает встроенный механизм обнаружения перехвата. Любое вмешательство в процесс передачи приводит к появлению ошибок в ключе, что позволяет сторонам обмена выявить факт атаки до использования ключевой информации.

В-третьих, квантовое распределение ключей позволяет формировать секретные ключи с высокой степенью доверия, потому что их безопасность может быть проверена в процессе передачи. Это особенно важно для систем, в которых критична защита каналов связи, включая государственные, финансовые и корпоративные сети.

Основной из проблем является высокая стоимость оборудования, включающего источники фотонов, детекторы и специализированные каналы связи. Существенным ограничением также является дальность передачи, поскольку потери сигнала в каналах связи снижают эффективность системы и усложняют ее интеграцию в существующую инфраструктуру. Дополнительные сложности связаны с требованиями к условиям функционирования квантовых систем: для сохранения стабильности квантовых состояний необходимо поддерживать строго контролируемые параметры среды, включая сверхнизкие температуры и защиту от внешних воздействий, так как любые помехи могут приводить к декогеренции. Кроме того, QKD используется совместно с классическими криптографическими алгоритмами и требует адаптации существующих систем информационной безопасности.

Заключение

Несмотря на существующие технические ограничения, технология имеет высокий потенциал практического применения. В перспективе развитие квантовых технологий и снижение стоимости оборудования будут способствовать более широкому внедрению QKD в системы защиты информации.

Квантовое распределение ключей – перспективное направление развития криптографической защиты информации, обеспечивающее высокий уровень безопасности за счет законов квантовой механики. В отличие от классических методов, QKD позволяет обнаруживать попытки перехвата и не зависит от вычислительных возможностей нарушителя, что делает его устойчивым к угрозам, связанным с развитием квантовых вычислений.

Список использованных источников

1. Что такое квантовая криптография. [Электронный ресурс] // Kaspersky Encyclopedia: Глоссарий. – URL: <https://encyclopedia.kaspersky.ru/glossary/quantum-cryptography/>. – Дата доступа: 15.03.2026.
2. Принципы работы некоторых квантовых протоколов шифрования. [Электронный ресурс] // Habr: Песочница. – URL: <https://habr.com/ru/sandbox/163613/>. – Дата доступа: 15.03.2026.

References

1. What is quantum cryptography [Electronic resource] // Kaspersky Encyclopedia: Glossary. – URL: <https://encyclopedia.kaspersky.ru/glossary/quantum-cryptography/>. – Access date: 03/15/2026.
2. Principles of operation of some quantum encryption protocols. [Electronic resource] // Habr: Sandbox. – URL: <https://habr.com/ru/sandbox/163613/>. – Access date: 15.03.2026.

Сведения об авторах

Савчук В.В., студентка факультета физики и информационных технологий, специальности «Кибербезопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», barbarasavchuk007@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by

Information about the authors

Savchuk V., student of the Faculty of Physics and Information Technology, specialty "Cybersecurity", Educational Institution "Francisk Skorina Gomel State University, Gomel", barbarasavchuk007@gmail.com

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Educational Institution "Francisk Skorina Gomel State University, Gomel", vaskevich@gsu.by

УДК 004.056

ОСНОВНЫЕ МЕРЫ ПО СНИЖЕНИЮ РИСКОВ SQL-ИНЪЕКЦИЙ

Е.Г. Ручаевская, Е.Д. Буйневич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь

Аннотация. В работе рассматривается проблема SQL-инъекций как одной из наиболее актуальных угроз информационной безопасности, сохраняющей лидирующие позиции в рейтинге OWASP несмотря на многолетнюю известность. Описаны механизмы реализации атак, потенциальные последствия вплоть до полной компрометации серверов баз данных. Предложен комплексный подход к защите, сочетающий

технические меры (параметризованные запросы, валидацию входных данных по принципу белых списков, разделение прав доступа, специализированные средства защиты) и организационные практики.

Ключевые слова: SQL-инъекции; уязвимость; вредоносный код; безопасность баз данных; запрос; параметризованные запросы; валидация данных; права доступа; средства защиты; программное обеспечение.

KEY MEASURES TO REDUCING THE RISKS OF SQL INJECTION

E.G. Ruchaevskaya, E.D. Buinevich

*Educational institution "Belarusian State University of Informatics and Radioelectronics" branch "Minsk Radio Engineering College",
Minsk, Republic of Belarus*

Abstract. The paper examines the problem of SQL injection as one of the most pressing threats to information security, which continues to hold a leading position in the OWASP ranking despite being known for many years. The mechanisms of attack implementation and the potential consequences, including complete compromise of database servers, are described. A comprehensive approach to protection is proposed, combining technical measures (parameterized queries, input validation based on the whitelisting principle, access right separation, specialized security tools) and organizational practices.

Keywords: SQL injection; vulnerability; malicious code; database security; query; parameterized queries; data validation; access rights; security tools; software.

Введение

Несмотря на то, что угроза SQL-инъекций известна сообществу разработчиков уже более двух десятилетий, она продолжает занимать лидирующие позиции в рейтинге опасностей OWASP (Open Web Application Security Project). SQL-инъекция – это метод внедрения злоумышленником вредоносных SQL-конструкций (ключевых слов или операторов) в поля ввода данных приложения. Успешная реализация такой атаки может привести к катастрофическим последствиям: от несанкционированного просмотра конфиденциальных данных (персональные данные, платежная информация) до полного уничтожения базы данных или получения злоумышленником административного контроля над системой [1].

Актуальность темы обусловлена тем, что многие современные приложения по-прежнему содержат уязвимый код, используют устаревшие фреймворки либо созданы с нарушением принципов безопасной разработки вследствие низкой квалификации разработчиков.

Основная часть

SQL-инъекции представляют собой класс уязвимостей, при которых вредоносный код внедряется в пользовательские входные данные для последующего выполнения на стороне сервера баз данных. Данный тип

атак нарушает семантику исходных запросов, что позволяет злоумышленнику обойти механизмы аутентификации и несанкционированно взаимодействовать с СУБД. Деструктивное воздействие SQL-инъекций может проявляться в различных формах: от инициирования ошибок приложения и переполнения буфера, ведущего к отказу в обслуживании, до несанкционированного повышения привилегий вплоть до уровня операционной системы.

Защита от SQL-инъекций не может быть обеспечена каким-то одним методом. Лучше всего применять как технические, так и организационные меры.

Одним из наиболее эффективных технических средств является использование параметризованных операторов, которые позволяют четко разделить логику SQL-запроса и пользовательские данные [2]. В подготовленном операторе структура запроса фиксируется заранее, а данные, полученные от пользователя, подставляются не через конкатенацию строк, а связываются с переменными. Благодаря этому при попытке SQL-инъекции внедренный код воспринимается не как исполняемая команда, а как строковое значение.

Однако, параметризованные операторы не обеспечивают защиту в случаях, когда требуется динамическое формирование имен таблиц или параметров сортировки. Поэтому ключевым дополнением к ним выступает валидация входных данных. Такой подход включает использование белых списков (разрешение только заранее определенных безопасных значений), проверку типа данных, ограничение длины полей ввода и контроль формата ввода.

Еще один важный принцип – минимизация прав доступа. Использование при подключении к базе данных учетной записи с правами администратора является грубой ошибкой. Для снижения рисков необходимо создавать для каждого приложения отдельную учетную запись, предоставляя ей строго минимально необходимые права, а также применять принцип разделения прав для отдельных модулей приложения.

Дополнительным барьером служат специализированные средства защиты. Программные или аппаратные решения анализируют входящий трафик и блокируют подозрительные запросы с признаками внедрения вредоносного кода еще до их передачи в приложение.

Нельзя забывать и о безопасности инфраструктурного слоя. Уязвимости могут возникать не только на уровне кода приложений, но и в самих системах управления базами данных, веб-серверах, а также в используемых фреймворках. Использование устаревшего программного обеспечения с известными уязвимостями делает все остальные меры защиты бессмысленными, поэтому своевременное обновление компонентов является критически важным.

Эффективная защита невозможна без систематического обучения разработчиков и администраторов принципам безопасного кодирования, а также без налаженного взаимодействия между командами разработки, информационной безопасности и администраторами баз данных. Практика применения библиотек и фреймворков, прошедших предварительную проверку со стороны службы информационной безопасности, позволяет снизить риск внесения уязвимостей на этапе разработки.

Заключение

SQL-инъекции остаются серьезной угрозой для информационной безопасности, однако, в отличие от многих сложных видов атак, они вполне предотвратимы. Эффективная стратегия защиты должна быть комплексной. Эффективная стратегия защиты должна быть комплексной и включать как технические меры, так и организационные практики. Такой подход не только повышает уровень защиты, но и ускоряет процессы разработки.

Список использованных источников

1. Карпиеня М.В. (2021) Защита веб-приложений от SQL-инъекций. Бизнес. Образование. Экономика : Международная научно-практическая конференция (Минск, 1-2 апр. 2021 г.), 163-165.
2. Кэмпбелл Л., Мейджорс Ч. (2020) Базы данных. Инжиниринг надежности. Санкт-Петербург, Издательство «Питер».

References

1. Karpienia M.V. (2021) Protection of Web Applications from SQL Injections. Business. Education. Economics: International Scientific and Practical Conference (Minsk, April 1-2, 2021), 163-165 (in Russian).
2. Campbell L., Majors C. (2020) Databases. Reliability Engineering. St. Petersburg, Piter Publishing (in Russian).

Сведения об авторах

Ручаевская Е.Г., канд. пед. наук, доц., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», elenruch@gmail.com.

Буйневич Е.Д., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», e.pulmanovskaya@gmail.com.

Information about the authors

Ruchaevskaya E., Cand. Sci. Ped., Associate Professor, teacher, educational institution "Belarusian State University of Informatics and Radioelectronics" branch "Minsk Radio Engineering College", elenruch@gmail.com.

Buinevich E., teacher, educational institution "Belarusian State University of Informatics and Radioelectronics" branch "Minsk Radio Engineering College", e.pulmanovskaya@gmail.com.

УДК 621.3.019.3

СТЕНДЫ ДЛЯ МОДЕЛИРОВАНИЯ ВОЗДЕЙСТВИЯ УДАРА НА РАДИОЭЛЕКТРОННЫЕ КОМПОНЕНТЫ

Г.В. Давыдов, И.Г. Давыдов, А.В. Потапович, В.А. Попов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Согласно нормативно-технической документации по испытаниям радиоэлектронной аппаратуры на одиночный удар нормируется значение ускорения ударного импульса и длительность ударного импульса. При этом требования по характеру изменения скорости движения испытуемого объекта, а также его перемещению в пространстве во время воздействия ударного импульса никоим образом не регламентируются. В работе показано, что игнорирование этими требованиями при выборе стендов для моделирования воздействия удара на радиоэлектронные компоненты может приводить к катастрофическим последствиям при эксплуатации.

Ключевые слова: одиночный удар, ускорение, скорость, перемещение, стенды моделирования удара.

STANDS FOR SIMULATING THE IMPACT EFFECT ON RADIOELECTRONIC COMPONENTS

H.V. Davydau, I.H. Davydau, A.V. Patapovich, V.A. Papou

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. According to regulatory and technical documentation for testing electronic equipment subject to single impacts, the shock pulse acceleration value and shock pulse duration are specified. However, requirements for the nature of the test object's velocity change, as well as its spatial movement during the impact of the shock pulse, are not regulated in any way. The paper demonstrates that ignoring these requirements when selecting test rigs for simulating the impact of shocks on electronic components can lead to catastrophic operational consequences.

Keywords: single strike, acceleration, speed, movement, strike simulation stands.

Введение

Работа посвящена анализу стендов для моделирования воздействия удара на радиоэлектронную аппаратуру и возникающие при этом различия

в несоответствии условий моделирования и реальных условий эксплуатации. Согласно нормативно-технической документации при испытаниях на одиночный удар нормируется значение ускорения ударного импульса и длительность ударного импульса, а зависимости для скорости и перемещения не нормируются.

Основная часть

Стенды для моделирования воздействия одиночных ударов на радиоэлектронную аппаратуру по принципу действия делятся на электродинамические, электромагнитные, гидравлические, пневматические, маятниковые, с падающей платформой, с падающим металлическим бойком на металлическую наковальню, с эксцентриковым механизмом, С точки зрения воспроизводства формы ударного импульса, скорости движения платформы, с испытуемым объектом, и перемещения платформы, ударные стенды имеют принципиальные различия. По форме ударного импульса все указанные стенды мало отличаются, за исключением амплитуды и длительности ударного импульса.

Стенды электродинамические, электромагнитные, гидравлические, пневматические характеризуются перемещением возвратно-поступательного характера с перемещениями в основном от 0.1 мм до 10 мм [1]. В начальный и конечный момент ударного импульса перемещение, скорость и ускорение равны нулю, т.е. имеет место состояние покоя. Если перемещение платформы происходит в одну сторону и обратно, то имеет место импульс. Скорость движения будет направлена в одну сторону и достигнет максимума, затем начнет уменьшаться и достигнет значения нуля. При этом перемещение будет иметь максимальное значение. Дальше начнется движение платформы в обратном направлении. Скорость будет направлена в обратном направлении, достигнет максимума, а затем начнет уменьшаться пока не станет равной нулю. При этом платформа стенда займет начальное положение.

Если рассматривать закон изменения скорости движения платформы т. е. ускорения, то будет иметь место два положительных максимума ускорения и один максимум отрицательного ускорения (ускорения в обратном направлении). Таким образом, для данных типов стендов характерно воспроизведение нескольких ударных импульсов, хотя за основной считается первый (максимальный по амплитуде) ударный импульс. Два других ударных импульса будут иметь меньшее ускорение и большую длительность.

Стенды маятниковые, с падающей платформой, с падающим металлическим бойком на металлическую наковальню, с эксцентриковым механизмом имеют другие соотношения по перемещениям, скоростям

и ускорениям для удара. При этом перемещения платформы происходит с одного положения в пространстве в другое, а скорость движения платформы равномерно нарастает до соприкосновения с ограничивающей поверхностью и при соприкосновении резко падает до нуля. Ударный импульс формируется при торможении платформы имеет форму похожую на полусинусоиду. Когда имеется отскок бойка от наковальни, то формируется при этом обратный импульс скорости. Как видно из рассмотренного анализа, принципиальные различия между двумя группами стендов заключаются в характере изменения скорости и перемещения платформы.

Если для первых типов стендов наличие зазоров между платформой и испытываемом изделием, а также наличие зазоров в самом изделии при воздействии удара приводит лишь к частичной ликвидации этого зазора за счет малых перемещений платформы то получается, что ускорение удара не передается на изделие или на элементы изделия. Для второй группы стендов, когда имеется даже незначительный зазор между платформой и испытываемым изделием, то вовремя удара происходит уменьшение зазора до его полного исчезновения и в результате чего происходит скачок изменения скорости соприкасающихся элементов и как результат значительное увеличения ударного импульса для испытываемого изделия. Экспериментальные исследования по влиянию не жесткого крепления транзисторов 2Т803 к бойку при испытании на удар с ускорением 12000g показали, что наличие зазоров приводит к катастрофическим отказам, хотя при жестком креплении амплитуда предельно-допустимых ускорений составляла 19000g.

Изделия, предназначенные для эксплуатации в условиях больших уровней одиночных ударных ускорений более 5000 g, должны быть сконструированы таким образом, чтобы отсутствовали люфты и зазоры в соединениях.

Заключение

При испытаниях изделий на одиночный удар следует использовать стенды, у которых ударный импульс формируется за счет резкой остановки движения платформы, а испытываемые изделия необходимо жестко крепить к платформе для исключения их перемещений при ударе.

Список использованных источников

1. Компьютерные технологии для расчета тепловых режимов и механических воздействий / Д.Ю. Муромцев, О.А. Белоусов; М-во образования и науки Рос. Федерации, Тамб. гос. техн. ун-т. - Тамбов: ТГТУ, 2012. - 87 с.

References

1. Computer technologies for calculating thermal conditions and mechanical effects / D.Yu. Muromtsev, O.A. Belousov; Ministry of Education and Science of the Russian Federation, Tambov State Technical University. - Tambov: TSTU, 2012. - 87 p. (in Russian).

Сведения об авторах

Давыдов Г.В., канд. техн. наук, доц., в. н. е., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Давыдов И.Г., канд. техн. наук, доц., доц. кафедры радиоинформационных технологий, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Потапович А.В., магистр, зав. НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Попов В.А., с. н. е., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Information about the authors

Davydau H.V., PhD, Leading researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil56@bsuir.edu.by.

Davydau I.H., PhD, Associate Professor at the Department Radioinformatics Technologies, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil56@bsuir.edu.by.

Potapovich A.V., Master of Technical Sciences, Head of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.

Papou V.A., researcher of SRL 5.3 of R&D department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.

УДК 621.382.2/.3

ПРИМЕНЕНИЕ ПЛАЗМОХИМИЧЕСКОГО ТРАВЛЕНИЯ В ОБРАТНОМ ИНЖИНИРИНГЕ ДЛЯ АНАЛИЗА АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

К.Н. Барковская, С.И. Мадвейко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В современном мире широкое применение находит метод обратного инжиниринга для обеспечения надежности элементной базы средств защиты информации. В данной статье описывается влияние технологии плазмохимического травления (ПХТ) полупроводниковых устройств как часть методики обратного инжиниринга. С помощью удаления слоев путем ПХТ можно выявлять дефекты и

вредоносные изменения в аппаратных средствах, что обеспечивает информационную безопасность.

Ключевые слова: обратный инжиниринг; плазмохимическое травление; плазма; травление; депроцессинг; интегральная схема; анализ; послойный анализ; потенциал плазмы; электрический потенциал.

APPLICATION OF PLASMA ETCHING IN REVERSE ENGINEERING FOR THE ANALYSIS OF HARDWARE INFORMATION SECURITY

K.M. Barkouskaya, S.I. Madveika

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. Nowadays the method of reverse engineering is widely used to ensure the reliability of the electronic components of information security tools. This article describes the impact of plasma etching technology of semiconductor devices as part of the reverse engineering methodology. By removing layers using plasma etching, defects and malicious changes in hardware can be identified, thereby ensuring information security.

Keywords: reverse engineering; plasma etching; plasma; etching; deprocessing; integrated circuit; analysis; layer by layer analysis; plasma potential; electric potential.

Введение

Интегральные схемы (ИС) обрабатывают большое количество информации, следовательно, возникает проблема возможности утечки конфиденциальной информации. Причиной утечки могут быть неисправные или скомпрометированные ИС, а также недостатки, преднамеренно внесенные в конструкцию злоумышленниками, которые называются аппаратными троянами. Подходы к обеспечению гарантии аппаратного обеспечения (hardware assurance) призваны гарантировать надежность этих устройств, подтверждая отсутствие в ИС вредоносных изменений.

На данный момент единственным надежным методом выявления троянов считается обратный инжиниринг (Reverse Engineering) – получение исходного аппаратного проекта путем разрушающего физического анализа готового продукта [1].

Поскольку современные ИС – это многослойные структуры, то для анализа архитектуры устройства и поиска дефектов необходимо открывать слои микросхемы. Данный процесс называется депроцессинг (deprocessing).

Депроцессинг включает две стадии: планаризацию (выравнивание поверхности) и послойное удаление материала. Для реализации этих процессов на практике применяют методы плазмохимического травления (ПХТ), химико-механической полировки, шлифовки и различные их комбинации [2].

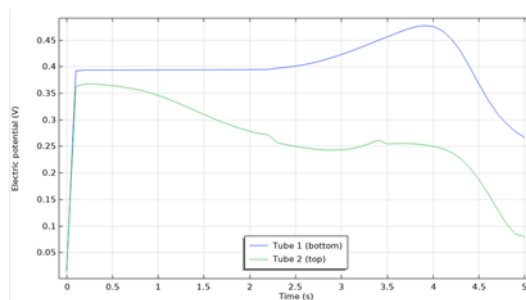
В данной статье будет рассмотрено влияние качества обработки методом ПХТ на точность послойного анализа.

Основная часть

Плазмохимическое травление – технология послойного удаления материала, основанное на химическом взаимодействии материала подложки с ионами плазмы. Травление применяется в процессе производства и изготовления электронной компонентной базы (ЭКБ), а также в операциях реверс инжиниринга ЭКБ [3]. Следовательно, развитие технологии ПХТ и модернизация соответствующего оборудования способствует повышению качества послойного анализа, а значит, возрастает степень защищенности данных.

Потенциал плазмы – одна из ее основных характеристик, которую рассматривают как электрическую потенциальную энергию, связанную с распределением этих заряженных частиц. Точное измерение и контроль потенциала плазмы необходимы для оптимизации плазменного оборудования. При травлении потенциал плазмы определяет энергию и направление ионов, влияя на скорость и селективность травления. Управление потенциалом плазмы позволяет настраивать условия плазмы для достижения желаемых результатов при травлении.

На рисунке 1 показана зависимость электронного потенциала плазмы от времени. Исследование проводилось для плазмы внутри двух камер.



Зависимость значения электрического потенциала от времени
The dependence of the electric potential value on time

Полученные результаты показывают, что значения электрического потенциала плазмы в трубках различается. Согласно рисунку, электрический потенциал более стабилен для камеры 1 (синяя линия), располагающейся в нижней части рабочей зоны, куда поступает меньше подводимой мощности, чем в камере 2 (зеленая линия), которая, наоборот, располагается в верхней части рабочей зоны и сюда поступает больше подводимой мощности. Таким образом, в камере 1 обработка более равномерная, а значит, точность послойного анализа возрастает.

Заключение

Стабильность значений электронного потенциала плазмы обеспечивает более равномерную обработку поверхности. На показатели электрического потенциала влияет распределение мощности внутри рабочей зоны.

Список использованных источников

1. Wilson R., Lu H., Zhu M., Forte D., Woodard D., Grieskamp W. (2021) REFICS: Assimilating Data-Driven Paradigms Into Reverse Engineering and Hardware Assurance on Integrated Circuits. *IEEE ACCESS*. 9, 131955–131976. DOI: 10.1109/ACCESS.2021.3114360.
2. Вяткин А. Ф., Зиненко В. И. (2012) Послойный анализ металлизации современных интегральных схем с помощью физического ионного распыления. *Известия вузов. Электроника*. 2 (94), 95–97.
3. Адамов А. А., Головки А. С., Малаханов А. А., Васильева Ю. О., Павлов А. В. (2024) Исследование скорости удаления пирогенного SiO₂ методом плазмохимического травления. *Автоматизация и моделирование в проектировании и управлении*. 4 (26), 4–11.

References

1. Wilson R., Lu H., Zhu M., Forte D., Woodard D., Grieskamp W. (2021) REFICS: Assimilating Data-Driven Paradigms Into Reverse Engineering and Hardware Assurance on Integrated Circuits. *IEEE ACCESS*. 9, 131955–131976. DOI: 10.1109/ACCESS.2021.3114360.
2. Vyatkin A. F., Zinenko V. I. (2012) Layer By Layer Analysis of Metallization in Modern Integrated Circuits Using Physical Ion Sputtering. *Proceedings of Universities. Electronics*. 2 (94), 95–97 (in Russian).
3. Adamov A. A., Golovko A. S., Malakhanov A. A., Vasil'eva Yu. O., Pavlov A. V. (2024) Investigating the Removal Rate of Pyrogenic SiO₂ by Plasma Chemical Etching. *Automation and modeling in design and management*. 4 (26), 4–11 (in Russian).

Сведения об авторах

Барковская К.Н., ассистент каф. электронной техники и технологии, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», k.barkovskaia@bsuir.by.

Мадвейко С.И., канд. техн. наук, доц., зав. каф. электронной техники и технологии, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», madveyko@bsuir.by.

Information about the authors

Barkouskaya K., Assistant at the Department of Electronic Technique and Technology, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, k.barkovskaia@bsuir.by.

Madveika S., Cand. of Sci. (Tech.), Associate Professor, Head of the Department of Electronic Technique and Technology, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, madveyko@bsuir.by.

УДК 004.056.5

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

М.Д. Юров, В.В. Чижик

*Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО», г. Минск, Республика Беларусь*

Аннотация. В работе анализируется современное состояние нормативно-правового регулирования в сфере информационной безопасности в Республике Беларусь. Рассматривается структура нормативной правовой базы в сфере информационной безопасности в Республике Беларусь. Особое внимание уделяется двенадцати основным нормативным правовым актам, определяющим обязательные для исполнения требования законодательства в сфере обеспечения кибербезопасности, в том числе технической и криптографической защиты информации. Приводятся статистические данные о состоянии киберпреступности в Республике Беларусь за 2025 год, подтверждающие актуальность исследуемой темы.

Ключевые слова: информационная безопасность; кибербезопасность; нормативно-правовое регулирование; нормативная правовая база; киберпреступления; национальная система кибербезопасности; Оперативно-аналитический центр при Президенте Республики Беларусь; информационная экономика; законодательство; Республика Беларусь.

NORMATIVE LEGAL REGULATION IN THE FIELD OF INFORMATION SECURITY IN THE REPUBLIC OF BELARUS

M. Yurau, V. Chizhik

*Higher Educational Establishment of the Federation of Trade Unions of Belarus
“International University “MITSO”, Minsk, Republic of Belarus*

Abstract. This paper analyses the current state of legal regulation in the field of information security in the Republic of Belarus. It examines the structure of the legal framework governing information security. Particular attention is paid to twelve key legal acts defining mandatory legislative requirements in the field of cybersecurity, including technical and cryptographic protection of information. Statistical data on the state of cybercrime in the Republic of Belarus for 2025 are presented, confirming the relevance of this topic.

Keywords: information security; cybersecurity; normative legal regulation; regulatory framework; cybercrime; national cybersecurity system; Operational and Analytical Center under the President of the Republic of Belarus; information economy; legislation; the Republic of Belarus.

Введение

В настоящее время в эпоху формирования информационной экономики уже можно констатировать тот факт, что данные, информация и знания становятся главным производительным ресурсом общества. В то же время активное развитие и внедрение информационно-коммуникационных технологий во все сферы жизнедеятельности способствует экспоненциальному росту объема информации, что создает как новые возможности для социально-экономического развития, так и дополнительные вызовы, связанные с обеспечением конфиденциальности, целостности и доступности информации.

В 2025 году в Республике Беларусь совершили порядка 20 тыс. киберпреступлений, что составило около 30 % от числа всех зарегистрированных случаев преступлений [1]. Данная статистика наглядно демонстрирует, что киберпреступность превратилась в масштабную угрозу социальной стабильности, экономическим интересам и национальной безопасности государства.

В этой связи в Республике Беларусь уже создана и активно совершенствуется нормативная правовая база в сфере информационной безопасности.

Основная часть

На сегодняшний день нормативная правовая база в области информационной безопасности в Республике Беларусь представлена через Конституцию Республики Беларусь, Трудовой кодекс Республики Беларусь, Кодекс Республики Беларусь об административных правонарушениях, Уголовный кодекс Республики Беларусь, 1 Решение Всебелорусского народного собрания, 1 Постановление Совета Безопасности Республики Беларусь, 7 Законов Республики Беларусь, 24 Указа Президента Республики Беларусь, 20 Постановлений Совета Министров Республики Беларусь, 7 Постановлений Оперативно-аналитического центра при Президенте Республики Беларусь, 40 Приказов Оперативно-аналитического центра при Президенте Республики Беларусь, 4 Приказа директора Национального центра защиты персональных данных Республики Беларусь, 2 Постановления Правления Национального банка Республики Беларусь, а также стандарты в области защиты информации.

Оперативно-аналитический центр при Президенте Республики Беларусь выделяет 12 основных нормативных правовых актов в сфере информационной безопасности:

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации».
2. Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет».
3. Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации».
4. Указ Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий».
5. Указ Президента Республики Беларусь от 14 февраля 2023 № 40 «О кибербезопасности».
6. Постановление Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)».
7. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г. № 60 «Об утверждении Положения о порядке определения уполномоченных поставщиков интернет-услуг».
8. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2010 г. № 92 «Об утверждении перечня уполномоченных поставщиков интернет-услуг».
9. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 65 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь».
10. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».
11. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 марта 2020 г. № 77 «О подтверждении соответствия средств защиты информации».
12. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» [2].

Заключение

Система регулирования охватывает ключевые аспекты информационной безопасности: защиту данных, кибербезопасность, интернет-услуги, сертификацию средств защиты информации, технические регламенты. Так, система законодательства продолжает развиваться, что отражает стремление государства адаптироваться к новым вызовам

цифровой среды. Государство последовательно формирует комплексную систему защиты информации, реагируя на рост цифровых угроз и увеличение числа киберпреступлений, которые уже составляют значительную долю от всех зарегистрированных преступлений.

В целом, Республика Беларусь выстраивает целостную и многоуровневую систему правового регулирования информационной безопасности, ориентированную на защиту государства, общества и граждан в условиях цифровизации.

Список использованных источников

1. Даревская В. От киберугроз до цифрового суверенитета: в Минске обсудили тему защиты персональных данных // Агентство «Минск-Новости». – 2026. – 28 янв. – URL: <https://minsknews.by/ot-kiberugroz-do-czifrovogo-suvereniteta-v-minske-obsudili-temu-zashhity-personalnyh-dannyh/> (дата обращения: 21.03.2026).

2. Рекомендации государственным органам и иным организациям (в том числе владельцам критически важных объектов информатизации) по выполнению обязательных для исполнения требований законодательства в сфере обеспечения кибербезопасности, в том числе технической и криптографической защиты информации // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: <https://www.oac.gov.by/public/content/files/files/recom.pdf> (дата обращения: 21.03.2026).

References

1. Darevskaya V., From cyber threats to digital sovereignty: the topic of personal data protection was discussed in Minsk // Minsk-Novosti Agency. – 2026. – January 28. – URL: <https://minsknews.by/ot-kiberugroz-do-czifrovogo-suvereniteta-v-minske-obsudili-temu-zashhity-personalnyh-dannyh/> (date of access: 21.03.2026).

2. Recommendations for government agencies and other organizations (including owners of critical information technology facilities) on the implementation of mandatory legislative requirements in the field of cybersecurity, including technical and cryptographic protection of information // Operations and Analysis Center under the President of the Republic of Belarus. – URL: <https://www.oac.gov.by/public/content/files/files/recom.pdf> (date of access: 21.03.2026).

Сведения об авторах

Юров М.Д., студент экономического факультета специальности «Управление информационными ресурсами», Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», maksimyurauscience@gmail.com.

Чижики В.В., старший преподаватель кафедры информационных технологий, Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», nest101999@mail.ru.

Information about the authors

Yurau M., student of the Faculty of Economics specialty "Information resources management", Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", maksimyurauscience@gmail.com.

Chizhik V., Senior Lecturer at the Department of Information Technology, Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", nest101999@mail.ru.

УДК 621.391.82

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТЕЧЕСТВЕННЫХ И ЗАРУБЕЖНЫХ СТАНДАРТОВ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

А.Д. Денскевич

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Проведен сравнительный анализ отечественных и зарубежных стандартов оценки разборчивости речи. Выявлены принципиальные различия в подходах: отечественные методы ориентированы на слоговую разборчивость с участием групп дикторов и аудиторов, зарубежные – на объективные физические индексы. Определены области применения каждого подхода для задач защиты речевой информации.

Ключевые слова: разборчивость речи; ГОСТ Р 50840-95; СТБ ГОСТ Р 50840-2000; STI; SII; артикуляционный метод; защита речевой информации; технические каналы утечки; инструментально-расчетный метод; оценка качества речи.

COMPARATIVE ANALYSIS OF DOMESTIC AND FOREIGN STANDARDS FOR SPEECH INTELLIGIBILITY ASSESSMENT IN INFORMATION SECURITY

A.D. Denskevich

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. A comparative analysis of domestic and foreign standards for assessing speech intelligibility has been carried out. Fundamental differences in approaches have been identified: domestic methods focus on syllabic intelligibility with the participation of groups of speakers and auditors, while foreign methods focus on objective physical indexes. The fields of application of each approach for the tasks of speech information protection are defined.

Keywords: speech intelligibility; GOST R 50840-95; STB GOST R 50840-2000; STI; SII; articulation method; speech information protection; technical leakage channels; instrumental-calculation method; speech quality assessment.

Введение

Оценка защищенности речевой информации от утечки по техническим каналам базируется на методах определения разборчивости речи [1]. Под разборчивостью понимается отношение количества правильно принятых элементов речи (слов, слогов, фраз) к общему числу произнесенных. В зависимости от цели используются различные подходы, регламентированные национальными и международными стандартами. Проведем сравнительный анализ отечественных и зарубежных стандартов оценки разборчивости речи применительно к задачам защиты информации.

Основная часть

В Российской Федерации основным нормативным документом оценки разборчивости речи является ГОСТ Р 50840-95, в Республике Беларусь – СТБ ГОСТ Р 50840-2000 [2, 3]. Стандарты устанавливают методы артикуляционных измерений, парных сравнений и фразовой разборчивости при ускоренном темпе.

Артикуляционный метод является экспериментален, та как в данном методе участвуют группы аудиторов и дикторов (не менее трех человек возраста 18–30 лет) [4]. В основе расчетных методов – разбиение речевого диапазона на 20 полос равной разборчивости; индекс артикуляции – сумма произведений весового коэффициента (0,05) на отношение сигнал/шум в полосе [1].

В международной практике распространены стандарты STI и SII. STI (IEC 60268-16) – индекс передачи речи, учитывает реверберацию, где значения оценки варьируются: 0–0,3 – плохая разборчивость, 0,3–0,6 – удовлетворительная, 0,6–1 – хорошая [5]. SII (ANSI S3.5-1997) – индекс разборчивости речи, подразумевающий развитие артикуляционного индекса, который основан на доле доступной слушателю информации в частотных полосах [6].

Отечественные стандарты ориентированы на слоговую разборчивость (диапазон 250–4000 Гц, реверберация не учитывается), учитывают особенности русского и белорусского языка. Зарубежные стандарты STI (125-8000 Гц, учет реверберации) и SII (20 полос, 80-8000 Гц) – объективные индексы, не привязаны к языку, не требуют экспертов, но в отечественной практике защиты информации применяются ограниченно. Отечественные методы имеют развитую нормативную базу и широко используются.

Однако существующие стандарты ориентированы на слуховое восприятие человека, тогда как современные средства перехвата используют алгоритмы машинного обучения. Зарубежные подходы также

не учитывают возможностей автоматического распознавания речи. Более детальный анализ мог бы включить расширенные числовые сопоставления и сравнение подходов, требующих углубленного исследования. Перспективным направлением является разработка критериев, учитывающих метрики WER и CER для ASR-систем.

Заключение

Отечественные стандарты (ГОСТ Р 50840-95, СТБ ГОСТ Р 50840-2000) базируются на артикуляционных измерениях с участием групп дикторов и аудиторов. Зарубежные (IEC 60268-16, ANSI S3.5-1997) предлагают объективные физические индексы, не требующие привлечения экспертов. Для задач защиты речевой информации предпочтительны отечественные методы, ориентированные на конкретный язык и имеющие развитую нормативную базу. Перспективным является разработка методик, учитывающих устойчивость речи к автоматическому распознаванию.

Список использованных источников

1. Давыдов, Г. В. Оценка разборчивости речи / Г. В. Давыдов, В. А. Попов, А. В. Потапович // Технические средства защиты информации : тезисы докладов XVIII Белорусско-российской научно-технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2020. – С. 24–25.
2. ГОСТ Р 50840-95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – М.: Издательство стандартов, 1995. – 234 с.
3. СТБ ГОСТ Р 50840-2000. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – Минск: Госстандарт, 2000. – 366 с.
4. Готовко, М. А. Оценка защищенности речевой информации / М. А. Готовко, Г. В. Давыдов, Е. Н. Сейткулов // Информационные технологии и системы 2013 (ИТС 2013) : материалы международной научной конференции, БГУИР, Минск, 23 октября 2013 г. – Минск, 2013. – С. 268–269.
5. IEC 60268-16:2020. Оборудование звуковой системы – Часть 16: Объективная оценка разборчивости речи по индексу передачи речи. – Женева: IEC, 2020. – 219 с.
6. ANSI S3.5-1997. Методы расчета индекса разборчивости речи. – Нью-Йорк: Акустическое общество Америки, 1997. – 36 с.

References

1. Davydov, G. V. Assessment of speech intelligibility / G. V. Davydov, V. A. Popov, A.V. Potapovich // Technical means of information protection : abstracts of the XVIII Belarusian-Russian Scientific and Technical Conference, Minsk, June 9, 2020 / Belarusian State University of Informatics and Radioelectronics. Minsk, 2020. pp. 24-25.
2. GOST R 50840-95. Speech transmission over communication paths. Methods of quality assessment, legibility and recognizability. – M.: Publishing House of Standards, 1995. – 234 p.

3. STB GOST R 50840-2000. Speech transmission over communication paths. Methods for assessing quality, legibility, and recognition. Minsk: Gosstandart Publ., 2000. 366 p.

4. Gotovko, M. A. Assessment of the security of speech information / M. A. Gotovko, G. V. Davydov, E. N. Seitkulov // Information technologies and systems 2013 (ITS 2013) : proceedings of the international scientific conference, BSUIR, Minsk, October 23, 2013 – Minsk, 2013. – pp. 268-269. 5. IEC 60268-16:2020. Sound system equipment – Part 16: Objective rating of speech intelligibility by speech transmission index. – Geneva: IEC, 2020. – 219 p.

5. IEC 60268-16:2020. Sound system Equipment – Part 16: Objective assessment of speech intelligibility by the speech transmission index. – Geneva: IEC, 2020. – 219 p.

6. ANSI S3.5-1997. Methods for Calculation of the Speech Intelligibility Index. – New York: Acoustical Society of America, 1997. – 36 p.

Сведения об авторе

Денскевич А.Д., ассистент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.denskevich@bsuir.by.

Information about the author

Denskevich A.D., assistant, Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail: a.denskevich@bsuir.by.

УДК 004.032.26

СРАВНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБРАБОТКИ РЕЧЕВЫХ СИГНАЛОВ

И.А. Коржова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе рассматривается применение рекуррентных нейронных сетей для обработки речевых сигналов. Проведено сравнительное исследование архитектур RNN, LSTM и GRU при анализе признаков речевых сигналов, полученных методом мел-частотных кепстральных коэффициентов (MFCC). Выполнено обучение моделей на наборе аудиоданных и проведена оценка качества их работы по метрикам точности и функции потерь. Полученные результаты позволяют определить эффективность различных архитектур рекуррентных нейронных сетей при обработке речевой информации и могут быть использованы при разработке систем анализа и защиты речевых данных.

Ключевые слова: Обработка речевых сигналов; Нейронные сети; Рекуррентные нейронные сети; RNN; LSTM; GRU; MFCC; Машинное обучение; Анализ речи; Защита информации.

COMPARISON OF RECURRENT NEURAL NETWORKS FOR SPEECH SIGNAL PROCESSING

I.A. Korzhova

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. This paper considers the application of recurrent neural networks for speech signal processing. A comparative study of RNN, LSTM and GRU architectures is carried out using speech features obtained by the Mel-Frequency Cepstral Coefficients (MFCC) method. The models are trained on a speech dataset and evaluated using accuracy and loss metrics. The obtained results allow assessing the effectiveness of different recurrent neural network architectures in speech signal processing and can be used in the development of speech analysis and information protection systems.

Keywords: Speech signal processing; Neural networks; Recurrent neural networks; RNN; LSTM; GRU; MFCC; Machine learning; Speech analysis; Information security.

Введение

Современные системы обработки речевых сигналов широко применяются в различных областях информационных технологий, включая системы распознавания речи, голосовые интерфейсы и средства анализа аудиоданных. Особую актуальность задачи обработки речевых сигналов приобретают в области технической защиты информации, где требуется анализ и обработка речевых данных для выявления возможных угроз безопасности.

Речевой сигнал представляет собой сложную временную последовательность, содержащую информацию о фонетических особенностях речи. Для эффективного анализа таких сигналов применяются методы извлечения признаков, одним из наиболее распространенных среди которых являются мел-частотные кепстральные коэффициенты (MFCC). Данные признаки позволяют представить аудиосигнал в компактной форме, удобной для дальнейшей обработки алгоритмами машинного обучения.

В последние годы для анализа последовательных данных активно применяются рекуррентные нейронные сети. К числу наиболее распространенных архитектур относятся классические рекуррентные сети (RNN), а также их модификации – Long Short-Term Memory (LSTM) и Gated Recurrent Unit (GRU). Эти модели способны учитывать временные зависимости в последовательностях данных, что делает их эффективными при обработке речевых сигналов.

Целью данной работы является сравнительный анализ эффективности различных архитектур рекуррентных нейронных сетей при обработке признаков речевых сигналов.

Основная часть

В рамках исследования была проведена сравнительная оценка эффективности рекуррентных нейронных сетей для обработки речевых сигналов.

В качестве исходных данных использовался открытый корпус речевых записей Common Voice (русскоязычный сегмент). Для проведения эксперимента была сформирована подвыборка объемом 300 аудиофайлов. Небольшой объем выборки обусловлен ограничениями вычислительных ресурсов и используется для демонстрационного сравнительного анализа архитектур. Данные были перемешаны и разделены на обучающую и тестовую выборки в соотношении 80/20. В качестве упрощенной задачи классификации, позволяющей провести сравнительную оценку архитектур, использовалась бинарная разметка на основе длины текстовой транскрипции: записи с длиной предложения менее 50 символов относились к классу 0, остальные – к классу 1.

Выбор длины текстовой транскрипции в качестве метки класса обусловлен тем, что данная характеристика косвенно отражает степень контекстной зависимости речевого сигнала. Длинные предложения содержат больше разнообразных фонетических окружений и требуют удержания контекста на более протяженных временных интервалах, что близко к условиям задачи выделения аллофонов, где контекст играет определяющую роль. Таким образом, способность нейронной сети различать фрагменты с разной длительностью контекста является необходимым условием для последующего решения целевой задачи – формирования базы аллофонов на основе речи конкретного диктора.

Предварительная обработка данных включала:

- приведение аудиосигналов к частоте дискретизации 16 кГц;
- извлечение признаков на основе мел-частотных кепстральных коэффициентов (MFCC);
- формирование входных последовательностей фиксированной длины.

В качестве признакового представления использовались MFCC-векторы размерности 40 на временной шаг. Для обеспечения единообразия входных данных все последовательности были приведены к длине 200 временных шагов путем обрезания или дополнения нулями.

Для решения задачи бинарной классификации были реализованы три архитектуры рекуррентных нейронных сетей:

- классическая рекуррентная нейронная сеть (RNN);
- сеть с долгой краткосрочной памятью (LSTM);
- рекуррентная сеть с управляемыми вентилями (GRU).

Каждая модель имела следующую структуру: рекуррентный слой с 64 скрытыми нейронами (batch_first=True), за которым следует полносвязный слой с 2 выходными нейронами. Для классификации использовался последний временной шаг выходной последовательности рекуррентного слоя.

Обучение моделей проводилось с использованием следующих параметров:

оптимизатор Adam с коэффициентом скорости обучения 0.001;
функция потерь CrossEntropyLoss;
размер батча 16;
количество эпох обучения 20.

В таблице представлены основные метрики качества классификации для исследуемых архитектур: доля правильных ответов (Accuracy), полнота (Recall), точность (Precision) и F1-мера. Все метрики приведены в макроусреднении (macro-average).

Сравнение эффективности архитектур
Comparison of architecture efficiency

Архитектура	Доля правильных ответов (Accuracy)	Полнота (Recall)	Точность (Precision)	F1-мера (F1-score)
RNN	0.70	0.70	0.77	0.68
LSTM	0.91	0.91	0.91	0.91
GRU	0.91	0.91	0.92	0.91

На рисунке представлена динамика функции потерь (loss) в процессе обучения для всех трех моделей. По оси абсцисс отложены эпохи обучения, по оси ординат – значение функции потерь.

Анализ полученных результатов позволяет сделать следующие наблюдения:

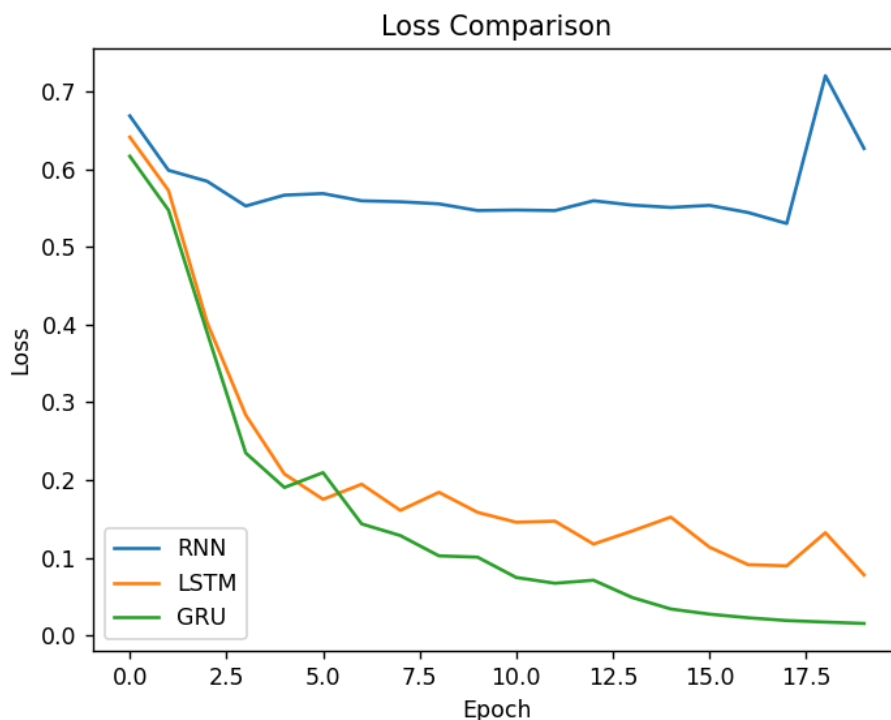
Модель RNN демонстрирует медленную сходимость и нестабильное поведение, что обусловлено проблемой исчезающего градиента, характерной для классических рекуррентных архитектур;

Модель LSTM характеризуется плавным и устойчивым снижением функции потерь, достигая высокой точности (91%) к 6-й эпохе;

Модель GRU обеспечивает наиболее быстрое снижение ошибки на ранних этапах обучения, показывая сопоставимые с LSTM финальные результаты (91 %).

Полученные результаты показывают, что классическая архитектура RNN уступает более современным модификациям при обработке речевых сигналов. Это связано с ограниченной способностью RNN учитывать

долгосрочные зависимости во временных рядах, что подтверждается теоретическими положениями, описанными в работах [1, 2].



Сравнение динамики функции потерь при обучении RNN, LSTM и GRU
Comparison of loss dynamics during training of RNN, LSTM and GRU

Модель LSTM продемонстрировала стабильное обучение и высокое качество классификации (Accuracy = 0.91). Благодаря механизму вентилей LSTM эффективно сохраняет контекстную информацию на протяжении длительных временных интервалов, что делает ее особенно подходящей для анализа речевых сигналов, характеризующихся сложной временной структурой.

Модель GRU показала сопоставимое качество с LSTM (Accuracy = 0.91) и более высокую скорость сходимости на начальных этапах обучения. Однако наблюдается более агрессивное снижение функции потерь, что может косвенно свидетельствовать о возможной склонности к переобучению при недостаточном объеме данных. Упрощенная архитектура GRU по сравнению с LSTM позволяет достичь сопоставимой точности при меньшем количестве параметров, что является преимуществом при ограниченных вычислительных ресурсах.

Заключение

В результате проведенного исследования установлено, что использование рекуррентных нейронных сетей позволяет эффективно обрабатывать речевые сигналы на основе MFCC-признаков.

Сравнительный анализ показал, что архитектуры LSTM и GRU значительно превосходят классическую RNN по всем рассмотренным метрикам точности и стабильности обучения. Модель LSTM обеспечивает наилучший баланс между точностью и стабильностью, в то время как GRU демонстрирует более быструю сходимость на начальных этапах обучения.

Полученные результаты могут быть использованы при разработке систем защиты речевой информации. В контексте формирования базы аллофонов и генерации акустических помех применение LSTM-архитектур позволяет создавать персонализированные речевые профили, которые могут применяться для защиты конфиденциальных переговоров путем наложения адаптированных аллофонных структур на речевой сигнал диктора. Это открывает перспективы для дальнейших исследований в области создания активных средств акустической защиты информации.

Список использованных источников

1. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. – Текст: электронный // Bioinf.jku.at: официальный сайт. – URL: <https://www.bioinf.jku.at/publications/older/2604.pdf> (дата обращения: 15.02.2025). 34 (2), 1–10.
2. Graves, A., & Schmidhuber, J. (2005). Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures. – Текст: электронный // Cs.toronto.edu: официальный сайт. – URL: https://www.cs.toronto.edu/~graves/nn_2005.pdf (дата обращения: 15.02.2025). 12 (3), 45–52.
3. Cho, K., et al. (2014). Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. – Текст: электронный // Arxiv.org: официальный сайт. – URL: <https://arxiv.org/abs/1406.1078> (дата обращения: 15.02.2025). 15 (4), 1–15.
4. Vaswani, A., et al. (2017). Attention Is All You Need. – Текст: электронный // Arxiv.org: официальный сайт. – URL: <https://arxiv.org/abs/1706.03762> (дата обращения: 15.02.2025). 30 (1), 1–15.
5. Panayotov, V., et al. (2015). LibriSpeech: An ASR Corpus Based on Public Domain Audio Books. – Текст: электронный // Arxiv.org: официальный сайт. – URL: <https://arxiv.org/abs/1506.02749> (дата обращения: 15.02.2025). 10 (2), 1–5.
6. Baevski, A., et al. (2020). wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations. – Текст: электронный // Arxiv.org: официальный сайт. – URL: <https://arxiv.org/abs/2006.11477> (дата обращения: 15.02.2025). 25 (3), 1–12.

References

1. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. – Text: electronic // Bioinf.jku.at: official web-site. – URL: <https://www.bioinf.jku.at/publications/older/2604.pdf> (date of request: 15.02.2025). 34 (2), 1–10.

2. Graves, A., & Schmidhuber, J. (2005). Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures. – Text: electronic // Cs.toronto.edu: official web-site. – URL: https://www.cs.toronto.edu/~graves/nn_2005.pdf (date of request: 15.02.2025). 12 (3), 45–52.

3. Cho, K., et al. (2014). Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. – Text: electronic // Arxiv.org: official web-site. – URL: <https://arxiv.org/abs/1406.1078> (date of request: 15.02.2025). 15 (4), 1–15.

4. Vaswani, A., et al. (2017). Attention Is All You Need. – Text: electronic // Arxiv.org: official web-site. – URL: <https://arxiv.org/abs/1706.03762> (date of request: 15.02.2025). 30 (1), 1–15.

5. Panayotov, V., et al. (2015). LibriSpeech: An ASR Corpus Based on Public Domain Audio Books. – Text: electronic // Arxiv.org: official web-site. – URL: <https://arxiv.org/abs/1506.02749> (date of request: 15.02.2025). 10 (2), 1–5.

6. Baevski, A., et al. (2020). wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations. – Text: electronic // Arxiv.org: official web-site. – URL: <https://arxiv.org/abs/2006.11477> (date of request: 15.02.2025). 25 (3), 1–12.

Сведения об авторах

Коржова И.А., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ikorzhova1@gmail.com

Information about the authors

Korzhova I.A., master student of the Department of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, ikorzhova1@gmail.com.

УДК 004.056:336.71(076)

УМЕНЬШЕНИЕ ОБЪЕМА ХРАНИМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБЕЗЛИЧИВАНИИ НА ОСНОВЕ МЕТОДА ИЗМЕНЕНИЯ СОСТАВА

А.М. Тимофеев¹, Д.В. Шляхтун²

¹*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

²*Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь*

Аннотация. В работе представлена процедура обезличивания персональных данных на основе метода изменения состава с акцентом на оптимизацию ресурсов хранения. Научная новизна заключается в использовании 9-битного кодирования алфавитно-цифровых символов, что позволяет исключить избыточное представление данных, характерное для UTF-16. Предложенный алгоритм не только обеспечивает высокий уровень информационной безопасности за счет изменения статистических свойств

персональных данных, но и уменьшает объем хранимых данных. Это делает процедуру эффективной для применения в крупномасштабных информационных системах с ограниченными дисковыми ресурсами.

Ключевые слова: информационные системы; персональные данные; защита информации; обезличивание персональных данных; методы обезличивания персональных данных; метод изменения состава.

REDUCING THE VOLUME OF STORED PERSONAL DATA BY DEPERSONALIZING IT BASED ON THE METHOD OF CHANGING THE COMPOSITION

Timofeev A.¹, Shliakhtun D.²

¹*Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus*

²*Educational Institution “National Children's Technopark”, Minsk, Republic of Belarus*

Abstract. This article presents a personal data anonymization procedure based on a compositional modification method with an emphasis on storage resource optimization. The scientific innovation lies in the use of 9-bit alphanumeric encoding, which eliminates the redundant data representation typical of UTF-16. The proposed algorithm not only ensures a high level of information security by modifying the statistical properties of personal data but also reduces the volume of stored data. This makes the procedure effective for use in large-scale information systems with limited disk resources.

Keywords: information systems; personal data; information protection; depersonalization of personal data; methods of depersonalization of personal data; method of changing the composition.

Введение

Одной из ключевых задач при создании современных информационных систем является обезличивание персональных данных [1 – 3]. Применяемые в настоящее время методы позволяют скрыть сведения от посторонних, сохраняя доступ к ним только для легитимных пользователей с помощью секретных параметров деобезличивания. Законодательство Республики Беларусь допускает использование метода изменения состава, который предполагает обобщение, модификацию или удаление идентифицирующей информации, для обезличивания персональных данных.

Однако традиционные подходы к реализации этого метода имеют недостатки: уязвимость перед статистическим анализом и необходимость выделения памяти для хранения измененных фрагментов. Более того, использование стандартных кодировок, например, UTF-16, создает избыточность, увеличивая нагрузку на инфраструктуру хранения и каналы передачи данных.

В данной работе представлена процедура обезличивания персональных данных на основе метода изменения состава, лишенная указанных недостатков. Предложенное решение ориентировано не только на модификацию статистических свойств персональных данных для повышения уровня их информационной безопасности, но и на значительное сокращение их объема.

Целью исследования являлась разработка процедуры обезличивания персональных данных, повышающей уровень их информационной безопасности и уменьшающей объем хранимых данных за счет оптимизации их бинарного представления. Объектом работы являлся метод изменения состава. Предметом исследования являлось повышение уровня информационной безопасности персональных данных с уменьшением используемого для их хранения объема баз данных.

Кодирование персональных данных

Предложенная процедура обезличивания персональных данных основана на переходе от стандартного шестнадцатибитного кодирования к оптимизированному девятибитному представлению символов. Это позволяет устранить структурную избыточность данных и уменьшить их объем для последующего хранения. Процесс подготовки информации заключается в преобразовании каждого символа исходного текста в компактный девятибитный блок. На основе анализа старшего байта исходного кода формируется бит-селектор: значение 0 соответствует кириллическому диапазону с префиксом 04, а значение 1 используется для латиницы и служебных знаков с префиксом 00. К сформированному флагу добавляется восьмибитное значение младшего байта символа. Переход к использованию девяти бит вместо шестнадцати обеспечивает сокращение объема хранимых данных на 43,7% в сравнении с исходным представлением в формате UTF-16.

Сформированная бинарная последовательность выравнивается до кратности шестидесяти четырем битам и подвергается криптографическому преобразованию методом наложения гаммы. Применение функции формирования ключа на основе пароля и добавления случайного шестнадцатибитного числа обеспечивает изменение статистических свойств данных, надежно защищая их от несанкционированного семантического анализа. Восстановление информации легитимным пользователем происходит путем расшифрования и декомпозиции потока блоками по девять бит. Алгоритм считывает бит-селектор, автоматически реконструирует соответствующий префикс и объединяет его с последующими восемью битами для получения исходного кода символа. Данный механизм исключает необходимость хранения дополнительных таблиц соответствия

или исходных фрагментов данных, так как вся информация для деобезличивания извлекается непосредственно из структуры девятибитных блоков. В результате предложенный метод позволяет существенно снизить требования к ресурсам систем хранения при обеспечении высокого уровня информационной безопасности.

Заключение

Разработана процедура обезличивания персональных данных на основе метода изменения состава, направленная на повышение уровня их информационной безопасности и оптимизацию ресурсов хранения.

В работе представлен способ 9-битного кодирования символов, позволяющий отказаться от избыточного представления данных. Предложенный подход обеспечивает снижение физического объема хранимых данных на 43,7% и сокращение длины соответствующих битовых потоков.

Список использованных источников

1. Ворона, В. А. (2023) *Биометрическая идентификация личности*. Москва, Горячая линия-Телеком.
2. Коллинз, М. (2020) *Защита сетей. Подход на основе анализа данных*. Москва, ДМК Пресс.
3. Остапенко, Г. А. (2020) *Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия*. Москва, Горячая линия-Телеком.

References

1. Vorona V. A. (2023) *Biometric Identification of Personality*. Moscow, Goryachaya Liniya-Telecom (in Russian).
2. Collins M. (2020) *A Data-Based Approach*. Moscow, DMK Press (in Russian).
3. Ostapenko G. A. (2020) *Information Operations and Attacks in Socio-Technical Systems: Organizational and Legal Aspects of Counteraction*. Moscow, DMK Press (in Russian).

Сведения об авторах

Тимофеев А.М., канд. техн. наук, доц., доц. каф. защиты информации, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», TAMvks@mail.ru

Шляхтун Д.В., учащаяся Учреждения образования «Национальный детский технопарк» по направлению «Информационная безопасность», rd2859002@gmail.com

Information about the authors

Timofeev A., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, TAMvks@mail.ru

Shliakhtun D., Student of the Educational Institution “National Children's Technopark” in “Information Security”, rd2859002@gmail.com

УДК 004.056.5:331.108(476)

КАДРОВЫЙ ПОТЕНЦИАЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

М.Д. Юров, В.В. Чижик

*Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО», г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается кадровый потенциал в сфере информационной безопасности Республики Беларусь в контексте формирования национальной системы обеспечения кибербезопасности. Проанализированы нормативно-правовые акты 2023–2025 гг., определяющие создание центров кибербезопасности и минимальную потребность в специалистах для их функционирования. Оценены возможности системы высшего образования по подготовке кадров в области информационной безопасности. Сопоставлены потребности и выпуск специалистов, что позволило определить степень обеспеченности отрасли квалифицированными кадрами и выявить существующие проблемы.

Ключевые слова: информационная безопасность; кибербезопасность; кадровый потенциал; подготовка специалистов; центры кибербезопасности; нормативно-правовые акты; кадровая потребность; критически важные объекты информатизации; национальная система кибербезопасности; система высшего образования.

HUMAN RESOURCE POTENTIAL IN THE FIELD OF INFORMATION SECURITY IN THE REPUBLIC OF BELARUS

M. Yurau, V. Chizhik

*Higher Educational Establishment of the Federation of Trade Unions of Belarus
“International University “MITSO”, Minsk, Republic of Belarus*

Abstract. The article examines the human resource potential in the field of information security in the Republic of Belarus within the framework of the development of the national cybersecurity system. The analysis covers regulatory acts adopted in 2023–2025 that define the establishment of cybersecurity centers and the minimum staffing requirements for their operation. The study assesses the capacity of the higher education system to train information security specialists. Compared the estimated personnel demand with the number of graduates, evaluated the sector's staffing sufficiency and identify existing issues.

Keywords: information security; cybersecurity; human resources; specialist training; cybersecurity centers; regulatory framework; staffing needs; critical information infrastructure; national cybersecurity system; higher education system.

Введение

Цифровая трансформация экономики и системы государственного управления Республики Беларусь обуславливает необходимость комплексного переосмысления подходов к обеспечению информационной безопасности как неотъемлемой составляющей национальной безопасности. В условиях расширения цифровой инфраструктуры, роста объемов обрабатываемых данных и усложнения киберугроз возрастает значимость формирования институциональных механизмов защиты информационного пространства государства.

Принятие Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности», а также последующих нормативных правовых актов, регламентирующих порядок его реализации, сформировало нормативно-правовую основу для построения национальной системы обеспечения кибербезопасности. Одним из ключевых структурных элементов данной системы выступают центры обеспечения кибербезопасности и реагирования на киберинциденты, создаваемые на объектах информационной инфраструктуры государственных органов и иных организаций (далее — центры кибербезопасности). Их деятельность направлена на мониторинг, предупреждение, выявление и нейтрализацию киберугроз, что обеспечивает повышение устойчивости национального цифрового пространства [1].

Основная часть

Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» установил, что 27 владельцев критически важных объектов информатизации, а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечивают создание центров кибербезопасности [1].

Постановление Совета Министров Республики Беларусь от 23 февраля 2024 г. № 120 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» определило перечень из 124 государственных органов и иных организаций, которые создают центры кибербезопасности и (или) приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры [1].

Постановление Совета Министров Республики Беларусь от 28 марта 2025 г. № 185 «Об изменении постановлений Совета Министров Республики Беларусь от 12 декабря 2023 г. № 879 и от 23 февраля 2024 г. № 120» определило перечень из 202 государственных органов и иных организаций, которые создают центры кибербезопасности и (или)

приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры [1].

Поскольку в общедоступных источниках есть только перечень из 33 аттестованных центров кибербезопасности, а информация по количеству неаттестованных центров кибербезопасности, как и по количеству сотрудников в них отсутствует, то предположим, что все организации в установленный срок создали центры кибербезопасности с минимальной численностью для прохождения аттестации, равной 11 штатным единицам, включая руководителя [2, 3]. На основании всего вышеперечисленного можно рассчитать минимальную кадровую потребность всех центров кибербезопасности за 2023-2025 гг., но без учета сотрудников Национального центра обеспечения кибербезопасности и реагирования на киберинциденты.

Таким образом, после проведения всех расчетов, получаем, что в 2023 году для обеспечения работы 27 центров кибербезопасности минимально требовалось 297 сотрудников, в 2024 году требовалось минимум 1364 сотрудника в 124 центра кибербезопасности, а в 2025 году требовалось минимум 2222 сотрудника для 202 центров кибербезопасности.

Теперь, когда мы установили минимальную кадровую потребность за 2023-2025 гг., необходимо выяснить достаточно ли специалистов готовят в учреждениях образования. На основании всего вышеперечисленного можно рассчитать максимально возможное количество специалистов, которые готовит система высшего образования за 2023–2025 гг. Важно отметить, что в данных расчетах не учитываются образовательные программы магистратуры, аспирантуры и докторантуры, поскольку в общедоступных источниках нет информации о планах приема за 2023-2025 гг.

После проведения всех расчетов, получаем, что в 2023 году на специальности бакалавриата по информационной безопасности готовили 409 бакалавров, из которых 293 обучались на бюджетной форме обучения, а 116 обучались на платной форме обучения, в 2024 году готовили 497 бакалавров, из которых 333 обучались на бюджетной форме обучения, а 164 обучались на платной форме обучения, в 2025 году готовили 409 бакалавров, из которых 277 обучались на бюджетной форме обучения, а 132 обучались на платной форме обучения [4].

Стоит упомянуть, что для более достоверных расчетов необходимо учитывать дополнительные факторы: текучесть кадров в сфере информационной безопасности, уход выпускников в другие сферы, трудоустройство сотрудников с непрофильным образованием, рост числа центров кибербезопасности в будущем и т.д.

Заключение

Проведенный анализ показал, что формирование национальной системы обеспечения кибербезопасности в Республике Беларусь сопровождается стремительным ростом потребности в квалифицированных кадрах. Минимальная кадровая потребность центров кибербезопасности увеличилась с 297 человек в 2023 году до 2222 человек в 2025 году, что соответствует среднегодовому темпу роста более 140 %. В то же время возможности системы высшего образования остаются ограниченными: ежегодный выпуск бакалавров по направлениям, связанными с информационной безопасностью колеблется в пределах 409–497 человек и не демонстрирует устойчивой тенденции к росту.

Сопоставление спроса и предложения свидетельствует о формировании значительного дефицита кадров, который в 2024–2025 гг. достиг 867 и 1813 человек соответственно. Коэффициент обеспеченности отрасли специалистами снизился до критического уровня – 18 % в 2025 году. Прогноз на 2026 год показывает дальнейшее увеличение дефицита при сохранении текущих тенденций.

Таким образом, существующая система подготовки кадров не обеспечивает потребности национальной системы кибербезопасности, что создает риски для устойчивого функционирования критически важной информационной инфраструктуры и реализации государственной политики в области информационной безопасности.

Список использованных источников

1. Национальный правовой Интернет-портал Республики Беларусь : [сайт]. – Мн., 2003–2026. – <https://pravo.by/> (дата обращения: 21.03.2026).
2. Перечень аттестованных центров кибербезопасности // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: <https://www.oac.gov.by/cybersecurity-centers-list/activity/certified-cybersecurity-centers> (дата обращения: 21.03.2026).
3. Рекомендации для создаваемых центров кибербезопасности // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: <https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-for-cybersecurity-centers> (дата обращения: 21.03.2026).
4. ИТ-абитуриент // Парк высоких технологий. – Мн., 2005–2026. – URL: <https://park.by/education/graduate/> (дата обращения: 21.03.2026).

References

1. National Legal Internet Portal of the Republic of Belarus: [website]. – Minsk, 2003–2026. – <https://pravo.by/> (date of access: 21.03.2026).

2. List of certified cybersecurity centers // Operations and Analysis Center under the President of the Republic of Belarus. – URL: <https://www.oac.gov.by/cybersecurity-centers-list/activity/certified-cybersecurity-centers> (date of access: 21.03.2026).

3. Recommendations for the creation of cybersecurity centers // Operations and Analysis Center under the President of the Republic of Belarus. – URL: <https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-for-cybersecurity-centers> (date of access: 21.03.2026).

4. IT applicant // Hi-Tech Park. – Minsk, 2005–2026. – URL: <https://park.by/education/graduate/> (date of access: 21.03.2026).

Сведения об авторах

Юров М.Д., студент экономического факультета специальности «Управление информационными ресурсами», Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», maksimyurauscience@gmail.com.

Чижи́к В.В., старший преподаватель кафедры информационных технологий, Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», nest101999@mail.ru.

Information about the authors

Yurau M., student of the Faculty of Economics specialty "Information resources management", Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", maksimyurauscience@gmail.com.

Chizhik V., Senior Lecturer at the Department of Information Technology, Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", nest101999@mail.ru.

УДК 004.056

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕТОДИКА ОЦЕНКИ КРИТИЧНОСТИ ИНЦИДЕНТА

О.А. Богушевич, А.С. Гайко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается проблема отсутствия законодательной классификации уровней опасности при утечке персональных данных в Беларуси. Предлагается авторская методика количественной оценки уровня угрозы, базирующаяся на балльной системе с учетом типа данных, масштаба утечки и отягчающих факторов. Разработан алгоритм реагирования для операторов в зависимости от установленного уровня критичности. Обосновывается необходимость принятия специализированного нормативного акта для повышения защиты прав субъектов персональных данных.

Ключевые слова: персональные данные; утечка данных; уровни опасности; защита информации; информационная безопасность; правовая неопределенность; балльная методика; критичность инцидента; алгоритм действий; классификация угроз.

LEAKAGE OF PERSONAL DATA: METHODOLOGY FOR ASSESSING THE CRITICALITY OF AN INCIDENT

O.A. Bogushevich, A.S. Gayko

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article addresses the lack of legally defined danger levels for personal data breaches in Belarus. A methodology for assessing incident criticality is proposed, featuring a scoring system and an action plan for operators. The need for a specialized regulatory act to strengthen the protection of personal data subjects' rights is justified.

Keywords: personal data; data breach; danger levels; data protection; information security; legal uncertainty; scoring methodology; incident criticality; response procedure; threat classification.

Введение

Цифровизация превратила персональные данные в ценный актив, а их утечку – в серьезную угрозу правам граждан. В Беларуси действует Закон «О защите персональных данных», однако он не содержит четких критериев оценки уровня опасности при инцидентах. Это создает правовую неопределенность для операторов и субъектов данных, затрудняя реагирование. Цель работы – анализ текущего регулирования и разработка практического алгоритма действий.

Основная часть

Действующее белорусское законодательство о защите персональных данных базируется на риск-ориентированном подходе. Закон «О защите персональных данных» обязывает операторов принимать меры защиты, соразмерные потенциальному вреду, однако само понятие «вред» и критерии его оценки не детализированы.

Анализ правовых норм позволяет выделить лишь косвенные признаки тяжести утечки: категория данных (обычные, специальные, биометрические), их объем и характер возможного ущерба. Утечка специальных категорий (данные о здоровье, религии, политических убеждениях) несет более высокие риски дискриминации, чем разглашение общедоступной информации. Но единой классификации уровней критичности в настоящее время не существует.

Это создает ряд проблем: у операторов нет ориентиров для реагирования и определения порога уведомления НЦЗПД; возникает субъективизм при расследовании; граждане не понимают серьезности угрозы при компрометации их данных.

Для решения предлагается внедрение балльной методики оценки уровня угрозы. Оператор оценивает три категории: тип утраченных данных (от 1 балла для технических до 10 баллов для специальных), объем

утечки (от 1 балла для 1–10 субъектов до 10 баллов для более 100 000) иотягчающие обстоятельства, которые суммируются. К последним относятся: публикация данных (+3), взлом (+2), отсутствие шифрования (+2), несамостоятельное обнаружение (+1), наличие данных несовершеннолетних или сведений о судимости (+2 за каждый пункт).

Итоговый уровень определяется суммой баллов: 1–5 – низкий, 6–12 – средний, 13–20 – высокий, 21 и более – критический. При утечке специальных категорий данных уровень автоматически признается критическим независимо от иных факторов.

План действий зависит от уровня угрозы. При низком уровне достаточно внутреннего расследования и устранения причин, уведомление НЦЗПД не требуется. При среднем необходимо локализовать инцидент, оценить последствия и рекомендуется уведомить регулятора. При высоком уровне требуется уведомление НЦЗПД в течение 72 часов, оповещение пострадавших и полное расследование. При критическом – уведомление регулятора в течение 24 часов, информирование МВД, публичное заявление и привлечение внешних экспертов.

Данный алгоритм устраняет правовую неопределенность: оператор, получив 15 баллов, понимает, что это высокий уровень, и обязан действовать соответственно – уведомить НЦЗПД в 72 часа и провести расследование, что снижает риски санкций за бездействие.

Заключение

Таким образом, утверждение об отсутствии в Беларуси требований по регуляции уровней опасности при утечке персональных данных является не совсем точным: общие принципы защиты и ответственности закреплены в законе. Однако отсутствие детализированной классификации и четких процедур реагирования на инциденты различной тяжести является существенным пробелом в праве. Предложенный в статье практический алгоритм, основанный на балльной системе оценки и конкретных планах действий, может служить основой для разработки ведомственного нормативного акта НЦЗПД. Внедрение такой методики является необходимым шагом для гармонизации белорусского законодательства с современными вызовами в сфере информационной безопасности и повышения уровня доверия граждан к цифровым сервисам и государственным институтам.

Список использованных источников

1. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь от 7 мая 2021 г. № 99-З // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: <https://pravo.by/document/?guid=3871&p0=N12100099>. – Дата доступа: 15.03.2026.

References

1. On Personal Data Protection [Electronic resource] : Law of the Republic of Belarus dated May 7, 2021 No. 99-Z // National Legal Internet Portal of the Republic of Belarus. – Mode of access: <https://pravo.by/document/?guid=3871&p0=H12100099>. – Date of access: 15.03.2026.

Сведения об авторах

Богушевич О.А., студент, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», rebenok1006@gmail.com.

Гайко А.С., студент, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», sanya040406@gmail.com.

Information about the authors

Bogushevich O.A., student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, rebenok1006@gmail.com.

Gayko A.S., student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, sanya040406@gmail.com.

УДК 623.094

СРЕДСТВА ЭЛЕКТРОМАГНИТНОГО ПОДАВЛЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А.М. Асиненко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматриваются современные средства электромагнитного подавления беспилотных летательных аппаратов (БПЛА). Представлен анализ трех основных типов систем противодействия: антидроновых ружей, стационарных комплексов и спуфинг-систем. Рассмотрены перспективы развития технологий противодействия БПЛА в контексте обеспечения безопасности объектов.

Ключевые слова: беспилотные летательные аппараты; БПЛА; средства подавления; радиоэлектронная борьба; антидрон-ружья; стационарные системы; спуфинг; электромагнитные помехи; защита объектов; системы безопасности.

MEANS OF ELECTROMAGNETIC SUPPRESSION OF UNMANNED AERIAL VEHICLES

A.M. Asinenko

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. The article discusses modern means of electromagnetic suppression of unmanned aerial vehicles (UAVs). It presents an analysis of three main types of countermeasure systems: anti-drone guns, stationary systems, and spoofing systems. The article also explores

the future development of UAV countermeasure technologies in the context of ensuring the security of facilities.

Keywords: unmanned aerial vehicles; UAVs; jamming equipment; electronic warfare; anti-drone guns; stationary systems; spoofing; electromagnetic interference; object protection; security systems.

Введение

Средства электромагнитного подавления беспилотных летательных аппаратов (БПЛА) – это комплексы РЭБ, блокирующие сигналы управления (2.4/5.8 ГГц), видеосвязи и GPS/ГЛОНАСС, вызывая посадку или возврат дрона.

Основные виды средств РЭБ против дронов:

– Антидрон-ружья (переносные). Компактные устройства, генерирующие направленный электромагнитный импульс. Примеры: REX-1, «Пищаль-ПРО», EDM4S.

– Стационарные системы. Создают «купол» (радиоэлектронное поле), защищающий объект (например, «Барьер РИ Купол», KRAKEN-M).

– Спуфинг-системы. Подменяют GPS-координаты, уводя дрон на ложную цель или вынуждая его приземлиться.

Основная часть

1 Антидроновое ружье – это мобильное средство РЭБ, подавляющее БПЛА на дистанциях до 1.5–2 км путем блокировки каналов управления, GPS/ГЛОНАСС и передачи видео. Устройство заставляет дрон сесть или вернуться на базу. Работает от аккумулятора, воздействуя на частотах 433 МГц – 5.8 ГГц.

Принцип работы основан на создании мощных радиопомех («шума») в зоне действия дрона, из-за чего тот теряет связь с оператором. Чем больше диапазонов поддерживает (обычно 900 МГц, 1.5 ГГц, 2.4 ГГц, 5.8 ГГц), тем выше эффективность против разных типов БПЛА. В среднем дальность действия от 500 метров до 2 километров. Преимущества:

– Компактность и простота использования.

– Сохранение целостности дрона (не физическое уничтожение, а посадка) [1].

2 Стационарные системы ЭМ-подавления БПЛА – это комплексы РЭБ для защиты инфраструктуры, создающие купол помех (360° или секторно) для разрыва каналов управления и GPS/ГЛОНАСС на дистанциях от 500 м до 5 км. Они работают круглосуточно, подавляя Wi-Fi, навигацию и сигналы управления.

Принцип действия основан на создании мощных помех в диапазонах, используемых дронами (МГц), что заставляет БПЛА зависать, приземляться или возвращаться на базу. Преимущества:

- высокая мощность и большая дальность подавления (до 2–5 км);
- защита от групповых атак.

Стационарные системы часто интегрируются с системами радиолокационного обнаружения для автоматического включения при приближении БПЛА [2].

3 Спуйфинг-системы (системы подмены сигналов) – это высокоэффективные средства борьбы с БПЛА, которые глушат реальные спутниковые сигналы (GPS/ГЛОНАСС) и замещают их ложными. Они заставляют дрон «думать», что он находится в другом месте, заставляя его отклониться от курса, принудительно сесть или зависнуть.

Принцип работы основан на том, что после обнаружения БПЛА система начинает транслировать более мощный сигнал, который «перебивает» реальные навигационные данные. Функционал систем подразумевает: блокировку старта, вмешательство в управление и принудительную посадку.

В отличие от простого «глушения» (Jamming), которое обрывает связь, спуйфинг дает ложные координаты, из-за чего БПЛА теряет ориентировку, но часто остается работоспособным, ожидая корректных данных [3].

Заключение

Проведенный анализ различных типов средств электромагнитного подавления беспилотных летательных аппаратов (БПЛА) позволяет сделать выводы об их эффективности и особенностях: выбор оптимального средства подавления БПЛА должен основываться на конкретных задачах защиты, характеристиках защищаемого объекта и имеющихся ресурсах. Наиболее перспективным направлением является развитие интегрированных систем, сочетающих различные методы подавления и обнаружения. При этом ключевым фактором успеха остается способность адаптироваться к постоянно эволюционирующим технологиям беспилотных летательных аппаратов.

В долгосрочной перспективе развитие средств подавления БПЛА будет определяться балансом между необходимостью обеспечения безопасности и требованиями к эффективности, мобильности и экономической целесообразности применяемых решений.

Список использованных источников

1. Антидрон пушки [Электронный ресурс]. – Режим доступа: <https://bezpeka.club/ru/top5-advantages-of-antidrone-guns>. – Дата доступа: 15.03.2026.
2. Стационарные комплексы радиоэлектронной борьбы [Электронный ресурс]. – Режим доступа: <https://antidrone.by/#:~:text=Стационарные%20комплексы%20>

радиоэлектронной%20,обратно%20в%20режим%20обнаружения%20беспилотников.. – Дата доступа: 15.03.2026.\

3. Спуфинг [Электронный ресурс]. – Режим доступа: <https://protectionsystem.ru/spoofing#:~:text=Спуфингом%20БПЛА%20называется%20глушение%20и,находится%20в%20совершенно%20другом%20месте..> – Дата доступа: 15.03.2026.

References

1. Antidrone cannons [Electronic resource]. – Access mode: <https://bezpeka.club/ru/top5-advantages-of-antidrone-guns>. – Access date: 15.03.2026.

2. Stationary electronic warfare systems [Electronic resource]. – Access mode: <https://antidrone.by/#:~:text=Stationary%20electronic%20warfare%20systems,back%20to%20drone%20detection%20mode..> – Access date: 15.03.2026.

3. Spoofing [Electronic resource]. – Access mode: <https://protectionsystem.ru/spoofing#:~:text=Spoofing%20UAV%20is%20called%20jamming%20and,is%20in%20a%20completely%20different%20place..> – Access date: 15.03.2026.

Сведения об авторах

Асinenko А.М., ассистент кафедры электронной техники и технологии, Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», a.asinenko@bsuir.by.

Information about the authors

Asinenka A., Assistant of the Department of Electronic Engineering and Technology, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, a.asinenko@bsuir.by.

УДК 004.056.52

ВНЕДРЕНИЕ МЕЖСЕТЕВОГО ЭКРАНА УРОВНЯ ПРИЛОЖЕНИЙ НА ПРЕДПРИЯТИИ

Н.А. Приходченко

Учреждение образования «Гомельский государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В данной статье рассматривается процесс выбора и внедрения межсетевого экрана уровня приложений (WAF) как критического компонента системы защиты современных веб-сервисов. Выделены основные трудности, с которыми сталкиваются предприятия при подборе средств защиты, включая разнообразие доступных на рынке решений и специфику нормативно-правовой базы Республики Беларусь. Описан пошаговый алгоритм, учитывающий соответствие техническим регламентам, особенности ИТ-инфраструктуры и квалификацию персонала предприятия. Практическая значимость работы заключается в систематизации этапов выбора, пилотного тестирования и настройки WAF для минимизации рисков и оптимизации затрат ресурсов.

Ключевые слова: межсетевой экран уровня приложений; WAF; информационная безопасность; веб-приложение; кибератака; алгоритм внедрения; ТР 2013/027/BY; фильтрация трафика; пилотное тестирование; защита данных.

IMPLEMENTATION OF A WEB APPLICATION FIREWALL AT AN ENTERPRISE

N.A. Pryknodchenko

*Educational Institution "Francysk Skaryna Gomel State University",
Gomel, Republic of Belarus*

Abstract. This article examines the process of selecting and implementing a Web Application Firewall (WAF) as a critical component of modern web service security systems. It highlights the key challenges enterprises face when selecting security solutions, including the diversity of solutions available on the market and the specifics of the regulatory framework of the Republic of Belarus. A step-by-step algorithm is described, taking into account compliance with technical regulations, IT infrastructure features, and staff qualifications. The practical significance of the work lies in the systematization of WAF selection, pilot testing, and configuration to minimize risks and optimize resource costs.

Keywords: Web Application Firewall; WAF; information security; web application; cyberattack; implementation algorithm; TR 2013/027/BY; traffic filtering; pilot testing; data protection.

Введение

На данный момент веб-приложения стали неотъемлемой частью современной информационной инфраструктуры. Также из-за своей выросшей важности они стали частой целью для кибератак, вследствие чего появилась острая необходимость в создании надежной системы защиты. Неотъемлемой частью такой системы является межсетевой экран уровня приложений (WAF) является неотъемлемым компонентом системы защиты веб-приложений. Этот инструмент выполняет фильтрацию HTTP/HTTPS трафика между сервисом и пользователем, защищает от ряда разновидностей атак, а также защищают сервисы API. Однако, несмотря на необходимость данного инструмента для безопасной работы приложений, выбор и внедрение межсетевого экрана уровня приложений на предприятии может стать сложной задачей для неподготовленных сотрудников. Эти трудности вызваны в первую очередь большим разнообразием вариантов WAF, доступных на рынке, а также особенностями его внедрения и сопровождения.

В этой статье описывается алгоритм выбора и внедрения WAF, призванный облегчить данные процессы для руководства и сотрудников фирм и предприятий.

Основная часть

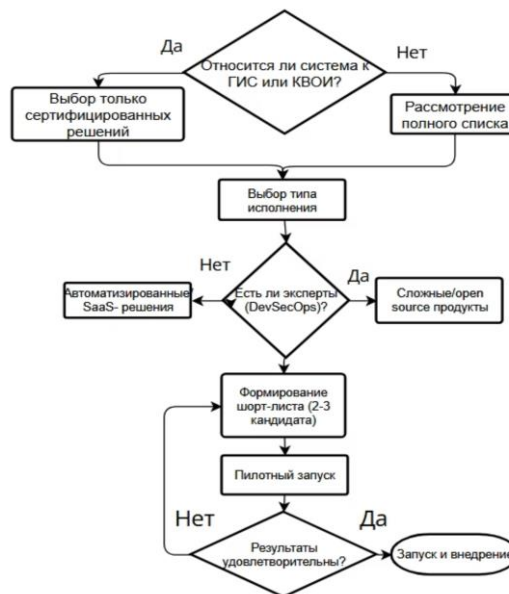
В первую очередь при выборе межсетевого экрана уровня приложений необходимо обеспечить соответствие нормативно-правовым документам в области информационной безопасности Республики Беларусь. Если защищаемая информационная система относится к критически важным объектам информатизации либо к государственным информационным системам (ГИС), то средства защиты должны иметь действующий сертификат соответствия требованиям Технического регламента ТР 2013/027/ВУ. В случае, если веб-приложение не относится к вышеуказанным информационным системам, наличие сертификата не является необходимым.

Вторым шагом будет рассмотрение архитектуры предприятия и наиболее вероятных угроз. Именно на этом этапе определяются желаемые характеристики WAF. Принятие решения на данном этапе во многом зависит от особенностей инфраструктуры, функций и вида деятельности конкретного предприятия.

На третьем этапе оценивается структура предприятия и его кадровый состав. Для большинства программных и аппаратных вариантов WAF необходимо наличие в штате квалифицированных специалистов, способных выполнить сопровождение и мониторинг во время работы системы защиты. В случае, если отдел информационной безопасности отсутствует либо не способен выполнить эту задачу, следует прибегнуть к использованию облачных межсетевых экранов, в случае которых сопровождение берет на себя провайдер услуги.

Заключительным этапом выбора WAF является пилотное тестирование. На этом шаге также начинается процесс внедрения межсетевого экрана в инфраструктуру предприятия. Непосредственно перед пробным запуском проводится подготовка среды. В течение срока от двух недель проводится тестирование WAF в режиме мониторинга, в ходе которого производится настройка и определяется эффективность работы средства защиты. Когда количество ложных срабатываний будет сведено к минимуму, WAF постепенно переводится в режим блокировки и интегрируется в существующую систему защиты предприятия. К этому моменту, как правило, уже принято окончательное решение о приобретении и внедрении межсетевого экрана. В случае, если в ходе пилотного тестирования средство защиты было признано неподходящим для предприятия, начинается повторный выбор продукта. Заключительным этапом внедрения является разработка регламентов эксплуатации, мониторинга и реагирования.

Основные шаги алгоритма представлены на рисунке.



Алгоритм выбора WAF для последующего внедрения на предприятии
Algorithm for WAF selection and subsequent enterprise implementation

Заключение

Из работы следует, что выбор WAF для последующего внедрения является сложной и комплексной задачей, требующей вдумчивого подхода и тщательного рассмотрения функций, рода деятельности, внутренней структуры и ресурсов предприятия. Внедрение неподходящего продукта может повлиять на работу всей инфраструктуры, снизить производительность работы либо привести к значительным финансовым и трудовым затратам. Представленный алгоритм выбора и внедрения должен облегчить выполнение данных задач и сэкономить ресурсы, которые в ином случае были бы потрачены напрасно.

Сведения об авторах

Приходченко Н.А., студент факультета физики и информационных технологий специальности «Компьютерная безопасность», Учреждения образования «Гомельский государственный университет имени Франциска Скорины», mbirann@gmail.com.

Information about the authors

Prykhodchenko N., student of the Faculty of Physics and Information Technology specialty “Computer security”, Educational Institution “Francysk Skaryna Gomel State University”, mbirann@gmail.com.

УДК 331.54

СОВЕРШЕНСТВОВАНИЕ ОТДЕЛЬНЫХ НОРМАТИВНЫХ АСПЕКТОВ ДЕЯТЕЛЬНОСТИ УПРАВЛЕНЧЕСКИХ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Гавришев

*Московский государственный лингвистический университет,
г. Москва, Россия*

Аннотация. Проведено исследование по усовершенствованию нормативных аспектов деятельности управленческих кадров по информационной безопасности (ИБ) на примере системы здравоохранения. Показано, что в указанной области имеется ряд нераскрытых нормативных вопросов. Приведены их примеры. Представлены отдельные предложения по совершенствованию нормативных аспектов деятельности управленческих кадров по ИБ в системе здравоохранения.

Ключевые слова: здравоохранение; заместитель руководителя; кадры; управление; деятельность; информационная безопасность; законодательство; нормативное регулирование; правовые акты, совершенствование.

IMPROVEMENT OF CERTAIN NORMATIVE ASPECTS OF MANAGEMENT PERSONNEL ON INFORMATION SECURITY

A.A. Gavrishev

Moscow State Linguistic University, Moscow, Russia

Abstract. A study has been conducted to improve the normative aspects of the activities of management personnel on information security (IS) using the example of the healthcare system. It is shown that there are a number of undisclosed regulatory issues in this area. Their examples are given. Separate proposals are presented to improve the normative aspects of the activities of management personnel on IS in the healthcare system.

Keywords: healthcare; deputy head; personnel; management; activities; information security; legislation; normative regulation; legal acts, improvement.

Введение

В современном мире управленческие решения играют решающую роль. Известно [4], что качество продуктов и услуг организаций любой формы собственности напрямую зависят от решений руководства. Несомненно, что это относится и к системе здравоохранения, которая является сегодня одной из наиболее важных социальных сфер любого общества [5].

Одним из новых направлений развития управленческих кадров в системе отечественного здравоохранения является управленческая деятельность по обеспечению информационной безопасности (ИБ) [1–3]. Согласно требованиям указа Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности

Российской Федерации», организации здравоохранения, являющиеся субъектами критической информационной инфраструктуры, обязаны делегировать полномочия по ИБ одному из заместителей руководителя. В целях соблюдения законодательных требований, Министерство Здравоохранения РФ выпустило письмо от 04.06.2022 г. № 18-4/И/2-9129 «О повышении устойчивости и безопасности функционирования информационных ресурсов Российской Федерации», подчеркивающее необходимость возложения ответственности за ИБ на заместителей руководителей таких учреждений, а также определяющее требования к их образованию и опыту.

Таким образом, на сегодняшний день управленческие кадры по ИБ стали неотъемлемой частью организационной структуры учреждений здравоохранения [1–3]. Исходя из этого, исследования в данной области являются актуальными и требуют дальнейшей проработки.

Основная часть

Рассмотрим некоторые результаты из известных источников, связанные с нормативными аспектами деятельности управленческих кадров по ИБ в системе здравоохранения. Так в документе «Методические рекомендации по формированию службы информационных технологий в медицинских организациях» (утв. ФГБУ «ЦНИИОИЗ» Министерства здравоохранения РФ 04.03.2022 г.) представлены рекомендации по формированию в медицинской организации службы информационных технологий (ИТ), предназначенной для обеспечения работоспособности, развития и модернизации ИТ и соответствующей инфраструктуры, интегрированных с единым цифровым контуром в здравоохранении. Однако указанный документ не регламентирует работу управленческих кадров по ИБ в системе здравоохранения. В работе [2] было проведено исследование рынка труда РФ, касающегося специалистов управленческого звена по ИБ медицинских организаций. Установлено, что в известных источниках данный вопрос освещается недостаточно подробно. Показано, что в России отсутствует, как устоявшаяся организационная структура, так и сформированный рынок труда в данном сегменте. Отмечается, что дефицит квалифицированных кадров по ИБ на рынке труда дополнительно усложняет процесс найма соответствующего персонала. Отмечено, что данный сегмент рынка труда РФ находится в стадии становления. В источнике [3] предлагается ряд мер по усовершенствованию нормативно-правовой базы, регламентирующей деятельность управленческого персонала по ИБ в сфере здравоохранения. Проведенный анализ показал, что действующая законодательная база в указанной области строится на основе федеральных законов, указов

Президента РФ и постановлений Правительства РФ. Однако существующие нормативные правовые акты (НПА) в данной области не включают специфических положений, учитывающих особенности сферы здравоохранения. Подчеркивается важность детализации этих аспектов в НПА Министерства здравоохранения РФ и других отраслевых подзаконных актах.

Из приведенных результатов видно, что в указанной области имеется ряд нераскрытых нормативных вопросов. Среди них, в первую очередь, отметим следующие [2, 3]:

- нет упоминания должности заместителя руководителя, ответственного за обеспечение ИБ, в НПА, регулирующих трудовые отношения в сфере ИБ;

- нет устоявшегося наименования должности заместителя руководителя медицинской организации, ответственного за обеспечение ИБ.

С учетом сказанного, предлагается усовершенствовать отдельные нормативные аспекты деятельности управленческих кадров по ИБ в системе здравоохранения с помощью следующих предложений [2, 3]:

- внести, с учетом требований законодательства, в отдельные профстандарты по ИБ, дополнение о должности заместителя руководителя организации, ответственного за обеспечение ИБ в организации, независимо от сферы ее деятельности. Указать наименование должности, должностные обязанности, требования к квалификации и пр.;

- нормативно закрепить типовое наименование должности заместителя руководителя медицинской организации, ответственного за обеспечение ИБ. По мнению автора, в качестве типового наименования такой должности возможно рассмотреть «Заместитель главного врача по информационной безопасности». Кроме этого, необходимо определить должностные обязанности, требования к квалификации, а также штатные нормативы для указанной должности.

Заключение

Таким образом, в данном докладе, проведено усовершенствование отдельных нормативных аспектов деятельности управленческих кадров по ИБ на примере системы здравоохранения.

Список использованных источников

1. Гавришев А.А. (2024) Исследование отдельных вопросов управления кадрами по информационной безопасности в медицинских учреждениях. *Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент»*. (1), 31–41.
2. Гавришев А.А. (2025) Нормативное регулирование деятельности управленческих кадров по информационной безопасности в сфере здравоохранения.

Территория новых возможностей. Вестник Владивостокского государственного университета. (3), 95-105.

3. Гавришев А.А. (2025) Состояние рынка труда в сегменте управленческих кадров по информационной безопасности учреждений здравоохранения. *Научный журнал НИУ ИТМО. Серия «Экономика и Экологический менеджмент».* (1), 123-133.

4. Деминг У.Э. (2006) Новая экономика. Москва, Эксмо.

5. Михайлова Ю.В., Мирошникова Ю. В., Князев А. А. (2014) Руководящие кадры органов и учреждений здравоохранения. *Вестник Росздравнадзора.* (6), 71-77.

References

1. Gavishev A.A. (2024) Research of certain issues of personnel management on information security in healthcare institutions. *Scientific journal NRU ITMO. Series "Economics and Environmental Management".* (1), 31–41.

2. Gavishev A.A. (2025) Normative regulation of the activities of management personnel on information security in the healthcare sector. *The Territory of New Opportunities. The Herald of Vladivostok State University.* (3), 95–105.

3. Gavishev A.A. (2025) The state of the labor market in the segment management personnel on information security for healthcare institutions. *Scientific journal NRU ITMO. Series "Economics and Environmental Management".* (1), 123–133.

4. Deming W.E. (2006) New Economy. Moscow: Eksmo.

5. Mikhailova Yu.V., Miroshnikova Yu.V., Knyazev A.A. (2014) Leading personnel of health authorities and institutions. *Bulletin of Roszdravnadzor.* (6), 71-77.

Сведения об авторах

Гавришев А.А., канд. техн. наук, доцент, Московский государственный лингвистический университет, alexxx.2008@inbox.ru.

Information about the authors

Gavishev A.A., Cand. Sci. (Tech.), Associate Professor, Moscow State Linguistic University, alexxx.2008@inbox.ru.

УДК 004.8; 004.056

ИСКУССТВЕННЫЙ ИММУНИТЕТ ЦИФРОВОЙ СРЕДЫ

А.О. Шустик, А.Ю. Савицкий

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Целью данной научной статьи является анализ актуальных методов противодействия фишинговым атакам с использованием технологий машинного обучения. В условиях экспоненциального роста числа мошеннических ресурсов традиционные сигнатурные методы обнаружения теряют эффективность. В статье рассматривается методика построения адаптивной системы обнаружения фишинговых сайтов, основанная на комплексном анализе URL-адресов, HTML-кода и визуальных признаков страниц. Представлен подход к классификации ресурсов с использованием ансамблевых методов машинного обучения, способных выявлять новые, ранее неизвестные угрозы в реальном времени. Результаты исследования демонстрируют

высокую практическую значимость для обеспечения безопасности финансового сектора и защиты персональных данных граждан.

Ключевые слова: кибербезопасность; обнаружение угроз; классификация веб-сайтов; анализ URL; ансамблевые алгоритмы; цифровая безопасность; фишинг; сторонний домен; черные списки; персональные данные.

ARTIFICIAL IMMUNITY OF THE DIGITAL ENVIRONMENT

A.O. Shustik, A.Yu. Savitsky

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The purpose of this research article is to analyze current methods for countering phishing attacks using machine learning technologies. With the exponential growth of fraudulent resources, traditional signature-based detection methods are becoming less effective. This article discusses a methodology for building an adaptive phishing site detection system based on a comprehensive analysis of URLs, HTML code, and visual characteristics of web pages. An approach to resource classification using ensemble machine learning methods capable of identifying new, previously unknown threats in real time is presented. The study's results demonstrate high practical significance for ensuring the security of the financial sector and protecting citizens' personal data.

Keywords: cybersecurity; threat detection; website classification; URL analysis; ensemble algorithms; digital security; phishing; third-party domain; blacklists; personal data.

Введение

Цифровые угрозы обгоняют развитие технологий. Фишинг перешел от простых писем к масштабным атакам, в которых присутствуют полные копии банковских и государственных порталов, точная имитация дизайна, URL и SSL-сертификатов. Количество подобных атак удваивается каждый год. Однако жизненный цикл мошеннического сайта на сегодняшний день не более четырех-шести часов. Тем не менее за это короткое время злоумышленники собирают данные десятков, иногда сотен пользователей, пока ресурс не попадет в черные списки. Стандартные методы блокировки не справляются с такой скоростью и динамикой угроз. Требуется новая система анализа, которая способна выявлять фишинг в реальном времени. Нужен интеллектуальный инструмент, который оценивает не только структуру страницы, но и поведение пользователя: путь навигации, задержки на элементах, движение мыши. Только такой подход выявляет аномалии до того, как жертва окажется в ловушке.

Основная часть

Срок жизни мошеннического сайта сокращается до 4–6 часов – это меняет приоритеты в защите. Здесь уже не столько важна частота обновлений черных списков, сколько скорость реакции. Система обнаружения фишинга, разработанная в рамках исследования, построена

по трехуровневой схеме: статический анализ атрибутов сайта сочетается с динамическим изучением поведения пользователя. Первый уровень – это фильтрация и сбор данных. Все начинается с извлечения признаков из URL, HTML-кода и визуальных особенностей страницы. Далее второй уровень, где реализовано ядро классификации на основе ансамблевых методов машинного обучения. Третий уровень – поведенческий – отслеживает действия пользователя: он проверяет решение, принятое на предыдущем этапе, или распознает атаку «нулевого дня», ускользнувшую от статического анализа.

Методология комплексного анализа признаков. Переход от оценки отдельных параметров к комплексному анализу разнородных данных стал основой нового подхода. Использование CatBoost в связке со стекингом, где логистическая регрессия выступает мета-алгоритмом, повышает точность классификации. Градиентный бустинг справляется с категориальными признаками без предварительного кодирования – это ускоряет обработку и позволяет работать в реальном времени.

Злоумышленники генерируют домены, чтобы обойти репутационные фильтры. В модели учитывают не только наличие известных брендов в URL, но и уровень хаотичности символов – фишинговые домены либо слишком упорядочены, либо, наоборот, чрезмерно хаотичны. Такие аномалии легко выявить по энтропии.

Подделка SSL-сертификатов – распространенная уловка. Поэтому в модель добавлены признаки за пределами базовой проверки: тип сертификата, дата выпуска, соответствие поля Subject Alternative Name реальному домену. Параллельно извлекают содержимое HTML-кода, чтобы найти признаки «кликджекинга» и подмены буфера обмена. Проверка показала: во всех 87 % фишинговых ресурсов с положительным результатом атрибут action форм указывает на сторонний домен – отличный от того, что отображается в браузере. Это свидетельствует о маскировке под доверенные сервисы.

Ансамблевые методы как инструмент противодействия новым угрозам. Традиционные модели машинного обучения, построенные на основе одного классификатора, показывают высокую точность при анализе исторических данных, однако теряют эффективность при появлении новых видов атак. Система решает эту проблему с помощью ансамбля из трех базовых алгоритмов: random forest обрабатывает разреженные признаки URL и сетевой инфраструктуры, catboost работает с категориальными характеристиками SSL и структурой HTML, сверточная нейронная сеть на архитектуре Siamese Networks сравнивает визуальное сходство подозрительной страницы с оригиналом. Мета-классификатор принимает финальное решение, обучаясь на вероятностных выходах базовых моделей. Эксперименты подтвердили,

что такой ансамбль выявляет ранее неизвестные угрозы с точностью 94,2%, что на 18% выше, чем у отдельных моделей. Разнообразие подходов компенсирует слабые стороны каждого алгоритма за счет их взаимодополняющих достоинств.

Поведенческий анализ в реальном времени. Система дополняет статический анализ поведенческим модулем. Он срабатывает при классификации ресурса как «подозрительного» по итогам статистики, а также при обнаружении SSL-сертификата и внешнего сходства с легитимным сайтом – таковы особенности современных фишинговых сценариев. Оцениваются три параметра взаимодействия. Время заполнения форм: фишинговые страницы почти не проверяют ввод на клиенте, что приводит к аномально быстрому вводу данных, несопоставимому с поведением при работе в настоящих банковских сервисах. Движение мыши: на подлинных сайтах оно плавное, целенаправленное. На поддельных – хаотичное или строго линейное, вызванное отсутствием привычной навигации или наличием скрытых iframe. Интервалы между действиями: отсутствие пауз на чтение или анализ информации указывает на автоматизацию или неосознанность действий. Такое поведение встречается почти исключительно в зараженных сессиях.

Заключение

Система обнаружения фишинга, основанная на адаптивных алгоритмах, анализирует URL, структуру HTML и визуальные элементы одновременно. Использование ансамблей моделей машинного обучения повышает точность выявления атак с кратким жизненным циклом от нескольких минут до двух часов. Включение метрик поведения пользователя: движения мышью, времени между переходами, последовательности навигации – устраняет ложные срабатывания на искусно сконструированные фейковые страницы. Подделки, имитирующие официальный дизайн и защищенные сертификатами SSL, перестают оставаться неуловимыми. Результаты экспериментов подтверждают эффективность подхода в реальных условиях особенно при защите финансовых платформ и персональных данных граждан.

Список использованных источников

1. Zhang, Y., Hong, J., Cranor, L. (2021). Cantina: A Content-Based Approach to Detecting Phishing Websites.
2. Marchal, S., et al. (2022). PhishStorm: Detecting Phishing With Streaming Analytics.
3. Д.П. Зегжда, Е.Б. Александрова, М.О. Калинин, И.Ю. Жуков, А.С. Марков. (2023). Кибербезопасность цифровой индустрии.

References

1. Zhang, Y., Hong, J., Cranor, L. (2021). Cantina: A Content-Based Approach to Detecting Phishing Websites.
2. Marchal, S., et al. (2022). PhishStorm: Detecting Phishing With Streaming Analytics.
3. D.P. Zegzhda, E.B. Aleksandrova, M.O. Kalinin, I.Yu. Zhukov, A.S. Markov. (2023). Cybersecurity of the digital industry.

Сведения об авторах

Шустик А.О., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lexa212110@gmail.com.

Савицкий А.Ю., канд. военн. наук, старший преподаватель кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», savialexey7@mail.ru.

Information about the authors

Shustik A., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lexa212110@gmail.com.

Savitsky A., Ph.D. in Military Sciences, Senior lecturer department of communications, Educational Institution "Belarusian State University of Informatics and Radioelectronics", savialexey7@mail.ru.

УДК 004.056.53; 004.8

АДАПТИВНОЕ ОБУЧЕНИЕ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ: ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И СТФ-ПЛАТФОРМ

К.Д. Янович, В.В. Васькевич

*Учреждение образования «Гомельский государственный университет
имени Франциска Скорины», г. Гомель, Республика Беларусь*

Аннотация. В данной работе предложена концепция адаптивной образовательной среды для подготовки специалистов по кибербезопасности, объединяющая технологии искусственного интеллекта и СТФ-платформ. Искусственный интеллект выступает в роли помощника: анализирует действия обучающегося, выявляет его слабые места и формирует индивидуальные практические задания. СТФ-платформы помогают закрепить полученные знания на практике. Такая концепция обеспечивает персонализированную траекторию обучения, повышает мотивацию и эффективность обучения и сокращает время подготовки специалистов, готовых к решению реальных задач защиты информационных систем.

Ключевые слова: адаптивное обучение; искусственный интеллект; кибербезопасность; СТФ-платформы; персонализация; индивидуальный маршрут; практические навыки; подготовка кадров; машинное обучение; образовательные технологии.

ADAPTIVE TRAINING OF CYBERSECURITY SPECIALISTS: USING AI AND CTF PLATFORMS

K.D. Yanovich, V.V. Vaskevich

*Educational Institution "Francisk Skorina Gomel State University",
Gomel, Republic of Belarus*

Annotation. In the article, the concept of an adaptive educational environment for training cybersecurity specialists is proposed, combining artificial intelligence technologies and CTF platforms. Artificial intelligence acts as an assistant: it analyzes the student's actions, identifies his weaknesses and forms individual practical tasks. CTF platforms help to consolidate the acquired knowledge in practice. This concept provides a personalized learning trajectory, increases motivation and learning efficiency, and reduces the training time for specialists who are ready to solve real-world information system protection tasks.

Keywords: adaptive learning; artificial intelligence; cybersecurity; CTF platforms; personalization; individual route; practical skills; staff training; machine learning; educational technologies.

Введение

В условиях современной реальности сфера кибербезопасности является одной из ключевых для обеспечения национальной безопасности, устойчивого развития бизнеса, государства и общества, а глобальный рынок испытывает острую нехватку квалифицированных специалистов. Поэтому обучение данных специалистов становится приоритетным и включает в себя как теоретическую базу, так и применение различных инструментов на практике, в том числе созданных на основе искусственного интеллекта (ИИ), а также CTF-площадок.

Основная часть

ИИ для обучения кибербезопасности имеет широкое применение. Данный инструмент может быть использован в качестве помощника для всех специалистов (начинающих или опытных) с целью обучения, помощи при решении различных задач, освоении инструментов или для сбора полезных источников. Он персонализирует контент под конкретного человека, а также сопровождает его на протяжении всего времени использования. Например, российская платформа Avareange, в которую входят индивидуальные маршруты обучения с учетом анализа поведения (используя ML и LangChain), чат-ассистент на базе нейросети GigaChat, моделирование фишинговых атак с автоматической корректировкой сценариев под опыт пользователя, прогнозирующая аналитика и построение планов CISO через систему Pulse (скоринг уязвимостей и OSINT), а также интерактивная панель с визуализацией уровня готовности персонала и динамики угроз. Центральная составляющая

решения – адаптивное обучение, основанное на технологиях искусственного интеллекта. Применение платформ LangChain и моделей машинного обучения дает возможность проводить глубокий анализ поведения сотрудников и формировать персонализированные образовательные подходы. Такой подход способствует повышению информированности команды об угрозах и эффективной подготовке к реалиям кибербезопасности [1].

Для опытных специалистов ИИ – мощный инструмент для проведения пентеста, который способен обрабатывать огромные объемы данных, выявлять шаблоны и автоматизировать сложные задачи, структурировать процессы отчетности. Также он позволяет повысить работоспособность специалистов, автоматизируя рутинные операции и помогая выявлять уязвимости, которые могут быть пропущены или незамечены при ручном тестировании [2]. Одним из ключевых направлений применения искусственного интеллекта в пентестах выступает эксплуатация уязвимостей. Современные ИИ-системы способны модифицировать готовые эксплойты или разрабатывать новые, ориентируясь на специфику целевой среды. Такой подход обеспечивает достоверную проверку наличия уязвимостей и снижает долю ошибочных срабатываний. Интеллектуальные платформы учитывают нюансы конфигурации системы и предлагают оптимальные способы подтверждения уязвимых мест.

В контексте обучения кибербезопасности, как было сказано ранее, важна не только теоретическая часть, но и практическая, в особенности практикоориентированность, поэтому платформы CTF (Capture The Flag) выступают связующим звеном между этими частями, позволяя применить полученные знания на практике. Там представлено множество различных категорий: OSINT, Forensics, PWN, Crypto, Web и другие. Основная цель данных платформ – «захватить флаг», то есть решить задания на определенные темы, ответом на которые выступает длинный код, состоящий из букв и цифр, зачастую обернутый в фигурные скобки. Примером таких платформ выступают площадки HackTheBox, TryHackMe, Codeby Academy и многие другие. Практикуясь в решении задач по различным темам, специалисты по кибербезопасности получают бесценный опыт для дальнейшей профессиональной карьеры, а также имеют возможность стать более конкурентноспособными на рынке труда.

Но не стоит забывать, что ИИ может использоваться как для обучения специалистами, так и злоумышленниками. ИИ также показывает высокий потенциал возможностей автоматизации компрометации защищаемой инфраструктуры. Оценка формируется на основе результатов тестирования ИИ в рамках программ Bug Bounty и соревнований типа CTF., например, в июне 2025 года ассистент Xbow занял лидирующую позицию в рейтинге HackerOne, выявив максимальное число уязвимостей в коде – что стало

историческим прецедентом для платформы. Система учитывает не только количество найденных багов, но и их критичность, анализируя безопасность программного обеспечения ведущих корпораций. Еще один случай – согласно исследованиям Palisade Research, агентный ИИ участвовал в CTF, где решил 19 из 20 заданий среди 400 команд, заняв позицию в топ-5% участников. На следующем этапе, в соревновании с участием почти 8000 команд, наиболее успешному ИИ-агенту удалось получить 20 флагов из 62, прочно войдя в Топ-10%. Недавно на темных форумах появились сообщения о новом инструменте Hexstrike-AI: он объединяет свыше 150 ИИ-агентов, способен автоматизированно проводить аудит инфраструктуры, эксплуатировать уязвимости, включая zero-day, и удерживать доступ в компрометированных системах – все это за считанные минуты. Подобные достижения наглядно демонстрируют высокий потенциал искусственного интеллекта, при этом его текущие успехи уже значительно превосходят те, которые были наблюдаемы всего год назад [3].

Заключение

Таким образом, применение ИИ и CTF-платформ для обучения специалистов по кибербезопасности имеет ключевую роль в качестве помощника для преподавателя, а не его замены.

Список использованных источников

1. Не учить, а адаптироваться. Российский стартап переизобрел тренировку по информационной безопасности с помощью ИИ. [Электронный ресурс] // Коммерсантъ. – 2025. – 28 августа. – URL: <https://www.kommersant.ru/doc/7989327>. – Дата доступа: 15.03.2026.
2. Огневчук, М. Как искусственный интеллект усиливает возможности специалистов по кибербезопасности. [Электронный ресурс] / М. Огневчук // Обзор ИИ-инструментов пентестов 2025. – 2025. – 4 июня. – URL: <https://www.h-x.technology/ru/blog-ru/review-ai-tools-pentest-2025-ru>. – Дата доступа: 15.03.2026.
3. Голушко, А. SOC будущего: ключевые тренды 2026-2028. [Электронный ресурс] / А. Голушко // Positive Technologies. – 2025. – 30 октября. – URL: <https://ptsecurity.com/research/analytics/the-future-soc-trends-defining-tomorrow-cyber-defense/#id2>. – Дата доступа: 15.03.2026.

References

1. Not to teach, but to adapt. A Russian startup has reinvented information security training using AI. [Electronic resource] // Kommersant. – 2025. – August 28. – URL: <https://www.kommersant.ru/doc/7989327>. – Access date: 15.03.2026.
2. Ognivchuk, M. How artificial intelligence enhances the capabilities of cybersecurity specialists. [Electronic resource] / M. Ognivchuk // Review of AI tools for pentests 2025. – 2025. – June 4. – URL: <https://www.h-x.technology/ru/blog-ru/review-ai-tools-pentest-2025-ru>. – Access date: 15.03.2026.

3. Golushko, A. SOC of the future: key trends 2026-2028. [Electronic resource] / A. Golushko // Positive Technologies. – 2025. – October 30. – URL: <https://ptsecurity.com/research/analytics/the-future-soc-trends-defining-tomorrow-cyber-defense/#id2> . – Access date: 15.03.2026.

Сведения об авторах

Янович К.Д., студентка факультета физики и информационных технологий, специальности «Кибербезопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», karifox100@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиопизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Yanovich K.D., student of the Faculty of Physics and Information Technologies, specialty "Cybersecurity", Education Institution "Francysk Skaryna Gomel State University", karifox100@gmail.com.

Vaskevich V.V., Senior Lecturer at the Department of Radiophysics and Electronics, Education Institution "Francysk Skaryna Gomel State University", vaskevich@gsu.by.

УДК 004.056.55

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: ПОЧЕМУ НАМ ПОРА МЕНЯТЬ МЕТОДЫ ЗАЩИТЫ

Д.С. Таран, В.А. Федоренко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье обсуждается, как развитие квантовых компьютеров ставит под удар привычную защиту данных. Старые алгоритмы (RSA, ECC), на которых держится почти весь интернет, скоро могут стать бесполезными из-за алгоритма Шора. Автор объясняет, почему нужно переходить на «постквантовые» методы защиты уже сейчас, и рассматривает один из самых крутых вариантов – криптографию на решетках. Также даются простые советы, как начать внедрять новую защиту в реальные системы.

Ключевые слова: криптография; квантовый компьютер; защита информации; шифрование; постквантовые алгоритмы; решетки; цифровая подпись; информационная безопасность; хакеры; алгоритм Шора.

POST-QUANTUM CRYPTOGRAPHY: WHY IT'S TIME TO CHANGE PROTECTION METHODS

D.S. Taran, V.A. Fedorenko,

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article discusses how the development of quantum computers threatens traditional data protection. Old algorithms (RSA, ECC), which support almost the entire

Internet, may soon become useless due to Shor's algorithm. The author explains why it is necessary to switch to "post-quantum" protection methods now and considers one of the coolest options – lattice-based cryptography. Simple tips are also given on how to start implementing new protection into real systems.

Keywords: cryptography; quantum computer; information security; encryption; post-quantum algorithms; lattices; digital signature; information security; hackers; Shor's algorithm.

Введение

Сегодня вся наша безопасность в сети – пароли, банковские карты, переписки – держится на криптографии. Мы привыкли думать, что это надежно, потому что обычному компьютеру нужны тысячи лет, чтобы подобрать ключ. Но скоро все изменится. Появляются квантовые компьютеры. Для них наши сложные математические задачи – это пустяк. Если мы не хотим, чтобы в один день все секреты мира были раскрыты, нам нужно срочно придумывать новые способы защиты – постквантовую криптографию.

Основная часть

Главная проблема в том, что квантовые компьютеры работают по другим законам физики. С помощью алгоритма Шора они могут мгновенно разламывать современные цифровые замки.

Что с этим делать? Математики предлагают использовать задачи, которые не под силу даже квантовому компьютеру. Самый перспективный вариант – это криптография на решетках.

Если говорить просто, то мы прячем секрет в огромной многомерной паутине из точек. Чтобы найти правильную точку, нужно решить уравнение:

$$As + e = b, \tag{1}$$

где A – матрица, s – секретный вектор, e – ошибка, b – правильная точка

В этой формуле вектор e играет роль намеренно внесенного шума. Даже небольшое отклонение делает невозможным использование стандартных методов решения линейных уравнений. Чтобы взломать такую защиту, злоумышленнику пришлось бы найти кратчайший вектор в многомерной решетке, что является NP -трудной задачей.

Помимо решеток, рассматриваются и другие методы защиты: криптография на основе хеш-функций, кодовая криптография.

Криптография на основе хеш-функций использует деревья Меркла для создания цифровых подписей. Стойкость здесь зависит только от надежности самой хеш-функции, а не от сложности теоретико-числовых задач. Это делает такие системы очень предсказуемыми и безопасными.

Кодовая криптография основана на использовании кодов, исправляющих ошибки (например, схема Мак-Элиса). Сообщение маскируется под случайный набор данных, и только владелец секретного ключа знает, как «исправить» этот шум и прочитывать исходный текст.

В настоящее время Национальный институт стандартов и технологий (NIST) уже завершает отбор алгоритмов, которые станут мировыми стандартами. Фаворитами выступают такие системы, как *CRYSTALS-Kyber* (для шифрования) и *CRYSTALS-Dilithium* (для цифровых подписей).

Переход на постквантовую защиту осложняется несколькими факторами. Во-первых, это размер ключей. Если классический ключ *RSA* может занимать 256–512 байт, то постквантовые ключи часто исчисляются килобайтами. Это создает дополнительную нагрузку на сетевые протоколы, такие как *TLS*, используемые при просмотре веб-страниц.

Во-вторых, возникает вопрос производительности. Постквантовые алгоритмы требуют больше оперативной памяти и ресурсов процессора. Это особенно критично для устройств интернета вещей (*IoT*) и мобильных гаджетов с ограниченным энергопотреблением.

Учитывая риски, эксперты предлагают использовать гибридный подход. Суть его в том, что данные шифруются одновременно двумя способами: старым (классическим) и новым (постквантовым). Если один из методов будет взломан, данные все равно останутся защищены вторым слоем. Это позволяет плавно внедрять новые технологии, не отказываясь от проверенных десятилетиями стандартов, пока квантовые компьютеры не стали массовой реальностью.

Заключение

Квантовая угроза – это не сюжет из кино, а реальность ближайших лет. Чтобы не остаться беззащитными, нужно уже сейчас тестировать гибридные системы (старая защита + новая). Это позволит плавно перейти на новые стандарты безопасности и не бояться появления мощных квантовых вычислителей.

Список использованных источников

1. Alagic, G. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / G. Alagic [et al.] // NIST Internal Report 8413. – 2022. – 54 p.
2. Алферов, А. П. Основы криптографии : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2005. – 480 с.

References

1. Alagic, G. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / G. Alagic [et al.] // NIST Internal Report 8413. – 2022. – 54 p.
2. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. (2005) Fundamentals of Cryptography: Tutorial. Moscow, Helios ARV (in Russian).

Сведения об авторах

Таран Д.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ulefol58@gmail.com

Федоренко В.А., начальник цикла кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.fedorenko@bsuir.by

Information about the authors

Taran D.S., cadet, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, ulefol58@gmail.com

Fedorenko V.A., Head of the cycle of the Department of Communications, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, v.fedorenko@bsuir.by

УДК 004.056:004.714

ОБРАЗОВАТЕЛЬНЫЙ ХАБ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

К.Ц. Маршалова, Е.А. Биюмен

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Описана концепция образовательного хаба в формате Point-and-Click для подготовки специалистов по защите информации. Обоснована эффективность геймификации и соревнований Capture The Flag (CTF) для повышения вовлеченности обучающихся. Разработанная на Unity архитектура включает получение заданий от неигровых персонажей (NPC) на локациях, мониторинг рейтинга в виртуальном хабе, а также экспорт артефактов на физический ПК для анализа в реальной операционной системе.

Ключевые слова: образовательная хаб; защита информации; геймификация; симулятор; Unity; Capture The Flag; кибербезопасность; NPC; практические навыки; интерактивная среда.

EDUCATIONAL HUB FOR TRAINING SPECIALISTS IN THE FIELD OF INFORMATION SECURITY

K.C. Marshalava, Y.A. Biyumen

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. The concept of an educational hab in the format of a Point-and-Click for training information security specialists is described. The effectiveness of gamification and Capture The Flag (CTF) competitions to increase student engagement is substantiated. The Unity-based architecture includes receiving tasks from NPCs, monitoring rankings in a virtual hub, and exporting artifacts to a physical PC for analysis in a real operating system.

Keywords: educational hab; information security; gamification; simulator; Unity; Capture The Flag; cybersecurity; NPC; practical skills; interactive environment.

Введение

Традиционные методы подготовки специалистов в области технической защиты информации зачастую не обеспечивают должного уровня вовлеченности обучающихся. Изучение криптографии, реверс-инжиниринга и сетевой безопасности требует непрерывной практики. Целью работы является создание интерактивной платформы в формате Point-and-Click, позволяющей обучающимся отрабатывать навыки отражения киберугроз и решения задач формата Capture The Flag (CTF) в симулированной среде, включающей взаимодействие с реальными информационными системами. В таблице представлена сравнительная характеристика традиционного метода обучения специалистов в области защиты информации и предложенного метода посредством интерактивной платформы, который отличается удобством использования, интерактивностью, масштабируемостью и наличием реальных примеров.

Сравнительная характеристика подходов к обучению
Comparative characteristics of learning approaches

Параметр оценки	Традиционное обучение	Геймифицированная 2D-платформа
Формат подачи материала	Лекции, статические стенды	Интерактивный сюжет, квесты от NPC
Мотивация обучающихся	Оценки, зачеты	Игровой прогресс, глобальный Leaderboard
Среда выполнения задач	Разрозненные виртуальные машины	Бесшовная интеграция игры и реальной ОС

Основная часть

Разрабатываемый хаб представляет собой интерактивный квест в жанре «Point-and-Click», реализованный на игровом движке Unity. Архитектура построена на модульной системе сцен, переход между которыми осуществляется с помощью скриптов обработки событий (UnityEvents) и 2D-коллайдеров. Игровой процесс стимулирует исследовательскую активность: практические задания («контракты»)

обучающийся получает через диалоги с неигровыми персонажами (NPC), распределенными по локациям игровой карты представленными на рисунке.

Центральным элементом навигации выступает виртуальная комната («хаб»). В ней реализован интерфейс персонального компьютера (личный кабинет), где обучающийся просматривает список активных заданий, сдает найденные «флаги» (через имитацию email) и отслеживает свою позицию в глобальном рейтинге (Leaderboard).

Ключевая особенность платформы – бесшовная интеграция игры с реальной практикой. Из комнаты обучающийся загружает тренировочные артефакты (сетевые дампы трафика, зашифрованные файлы) на свой физический компьютер. Решение задач происходит в реальной операционной системе с использованием подлинных утилит анализа защищенности.



Локации образовательного хаба
Educational Hub locations

Заключение

Разработанная платформа демонстрирует высокий потенциал геймификации в профильном образовании. Интеграция реальных инструментов защиты информации в логику 2D-квеста трансформирует традиционное обучение в увлекательный процесс расследования. Внедрение таких систем повышает качество подготовки, сокращает время адаптации к рабочим задачам и формирует интерес к самостоятельному поиску уязвимостей.

Список использованных источников

1. Шелупанов А. А., Мещеряков Р. В., Нахабов А. С. (2021) Геймификация в образовательном процессе подготовки специалистов по защите информации. Безопасность информационных технологий. 28 (2), 115–125.
2. Гаврилюк Е. Ю., Свалова А. С., Гончар В. Н. (2020) Применение инструментов имитационного моделирования при оптимизации образовательных процессов. (11), 49–53.

References

1. Shelupanov A. A., Meshcheryakov R. V., Nakhabov A. S. (2021) Gamification in the Educational Process of Training Specialists in Information Security. IT Security. 28 (2), 115–125 (in Russian).
2. Gavriluk E. Yu., Svalova A. S., Gonchar V. N. (2020) Application of Simulation Modeling Tools in Optimizing Educational Processes. (11), 49–53 (in Russian).

Сведения об авторах

Маршалова К.Ц., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», krissmarshalova@gmail.com.

Биюмен Е.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», eugene.aether@gmail.com.

Information about the authors

Marshalava K., student of Information Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", krissmarshalova@gmail.com.

Biyumen Y., student of Information Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", eugene.aether@gmail.com.

УДК 004.056.5

КЛАССИФИКАЦИЯ ТИПА СХЕМЫ В ПРОТОКОЛАХ ДВУСТОРОННИХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ АНАЛИЗА ТРАНСКРИПТА

Д.А. Руденок, У.А. Змачинская

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе исследуется определение типа логической схемы в протоколах 2PC (гарблированные схемы Яо) по транскрипту. На основе оптимизаций free-XOR и point-and-permute определены характерные размеры пакетов и задержки для гейтов AND и XOR. Сгенерированы транскрипты четырех реальных схем (mult2_64, AES-128,

SHA-256, FP-mul) с высоким уровнем шума и вариативности. Классификаторы Random Forest, логистическая регрессия и SVM достигли точности 99,9%. Это свидетельствует о существенной утечке информации о структуре функции, подтверждая необходимость разработки Function-Hiding MPC, скрывающей не только данные, но и логику вычислений.

Ключевые слова: гарблированные схемы Яо; безопасные двусторонние вычисления; классификация транскрипта; машинное обучение.

CLASSIFICATION OF CIRCUIT TYPE IN TWO-PARTY COMPUTATION PROTOCOLS BASED ON TRANSCRIPT ANALYSIS

D. Rudenok, U. Zmachynskaya

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. This study examines determining circuit type in Yao's 2PC protocols from transcripts. Based on free-XOR and point-and-permute optimizations, characteristic packet sizes and delays for AND and XOR gates were determined. Transcripts of four real circuits (mult2_64, AES-128, SHA-256, FP-mul) were generated with high noise and variability. Random Forest, logistic regression, and SVM classifiers achieved 99,9% accuracy. This indicates significant leakage of function structure, confirming the need for Function-Hiding MPC that conceals both data and computation logic.

Keywords: Yao's garbled circuits; secure two-party computation; transcript classification; machine learning.

Введение

Современные протоколы безопасных двусторонних вычислений (2PC) позволяют двум сторонам совместно вычислить функцию от их приватных входов, не раскрывая сами входы друг другу. Фундаментальная конструкция – гарблированные схемы Яо [1] – обеспечивает безопасность в модели получестного противника. Однако в реальных приложениях функция также может быть конфиденциальной (например, формула кредитного скоринга или диагностический алгоритм). Это привело к развитию направления Function-Hiding MPC (FH-MPC), где скрывается не только вход, но и сама вычисляемая функция [2].

Однако протоколы могут оставлять побочные следы (размеры пакетов, задержки), зависящие от структуры схемы (числа AND/XOR гейтов). Эти следы могут быть использованы для определения типа функции. В данной работе исследуется классификация типа схемы (AND или XOR) по статистическим признакам транскрипта.

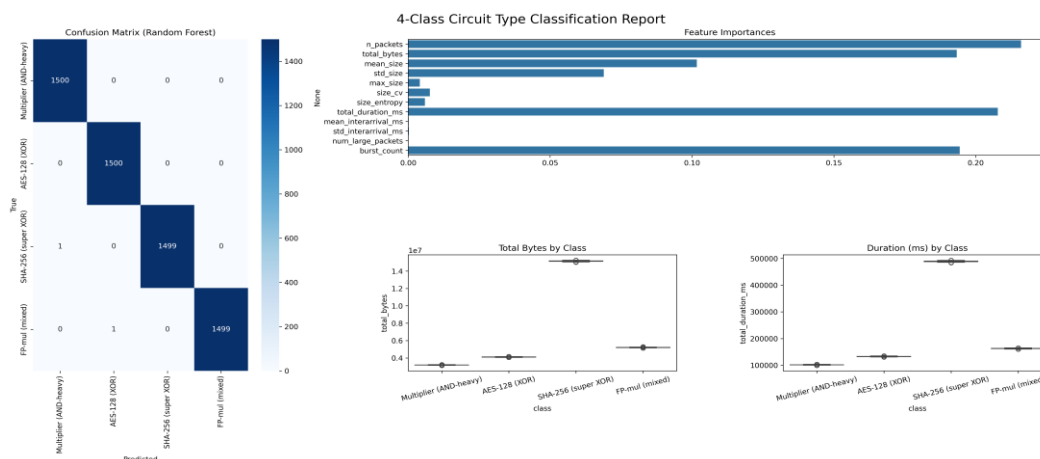
Основная часть

В данной работе рассматривается классический протокол Яо с оптимизациями free-XOR и point-and-permute [3]. Гарблер строит булеву схему из гейтов AND и XOR. XOR не требуют передачи таблиц и обрабатываются быстро, каждый AND порождает 4 зашифрованных записи (16 байт) [4], что увеличивает трафик и время выполнения. Противник может извлечь из транскрипта признаки, коррелирующие с типом схемы.

Размеры пакетов и задержки выбраны на основе характеристик гарблированных схем. Для AND задан диапазон 60–68 байт (4 записи с заголовками), для XOR – 14–18 байт (служебный трафик) [3,5]. Временные задержки основаны на [1]: обработка AND занимает 4 мкс, XOR – практически мгновенно; в модели средняя задержка AND 0.15 мс, XOR 0.10 мс, отражая соотношение сложности и сетевые вариации.

Вместо двух классов с искусственными вероятностями использованы четыре реальные схемы из бенчмарков Bristol Fashion: mult2_64 (AND-богатая), AES-128, SHA-256 (XOR-богатые) и FP-mul (смешанная). Длина схем варьируется от сотен до тысяч гейтов. Транскрипты сгенерированы с высоким шумом (20% случайных замен гейтов), вариативностью размеров и задержек, добавлением служебных пакетов и WAN-задержек. Сгенерировано по 1500 примеров на класс. Из каждого транскрипта извлекались: количество пакетов, суммарный объем данных, статистики размеров и интервалов, энтропия, длительность.

Применены Random Forest, логистическая регрессия и SVM с RBF-ядром.



Матрица ошибок классификации четырех типов схем (Random Forest). Классы: 0 – mult2_64, 1 – AES-128, 2 – SHA-256, 3 – FP-mul
Confusion matrix of four circuit types (Random Forest). Classes: 0 – mult2_64, 1 – AES-128, 2 – SHA-256, 3 – FP-mul

Заключение

Эксперимент показал: на четырех реальных схемах (mult2_64, AES-128, SHA-256, FP-mul) все модели (Random Forest, логистическая регрессия, SVM) достигли точности 99,9%. Наибольший вклад в предсказания Random Forest внесли средний размер пакета, длительность и объем данных. Результаты демонстрируют утечку информации о структуре схемы через транскрипт, обосновывая необходимость создания механизмов защиты Function-Hiding MPC.

Список использованных источников

1. Wang X., Malozemoff A. J., Katz J. (2016) Faster two-party computation secure against malicious adversaries in the single-execution setting. *Cryptology ePrint Archive*, 3–5.
2. Yao A. C. (1982) Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. 160–164.
3. Kolesnikov V., Schneider T. (2008) Improved garbled circuit: Free XOR gates and applications. *International Colloquium on Automata, Languages, and Programming*. 486–498.
4. Zahur S., Rosulek M., Evans D. (2015) Two halves make a whole. *Advances in Cryptology EUROCRYPT*. 220–250.
5. Rosulek M., Roy L. (2021) Three halves make a whole? Beating the half-gates lower bound for garbled circuits. *Advances in Cryptology – CRYPTO*. 2021. 3–32.

References

1. Wang X., Malozemoff A. J., Katz J. (2016) Faster two-party computation secure against malicious adversaries in the single-execution setting. *Cryptology ePrint Archive*, 3–5.
2. Yao A. C. (1982) Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. 160–164.
3. Kolesnikov V., Schneider T. (2008) Improved garbled circuit: Free XOR gates and applications. *International Colloquium on Automata, Languages, and Programming*. 486–498.
4. Zahur S., Rosulek M., Evans D. (2015) Two halves make a whole. *Advances in Cryptology EUROCRYPT*. 220–250.
5. Rosulek M., Roy L. (2021) Three halves make a whole? Beating the half-gates lower bound for garbled circuits. *Advances in Cryptology – CRYPTO*. 2021. 3–32.

Сведения об авторах

Змачинская У.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», u.grazhdano4ka@gmail.com.

Руденок Д.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», diorud92@yahoo.com.

Information about the authors

Zmachynskaya U., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", u.grazhdano4ka@gmail.com.

Rudenok D., student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", diorud92@yahoo.com.

УДК 004.056:355

ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Д.Г. Муравицкий, В.А. Федоренко

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматриваются особенности обеспечения информационной безопасности в условиях проведения специальной военной операции. Анализируются основные угрозы информационным системам и каналам связи, возникающие при активном применении средств радиоэлектронной борьбы, разведки и информационно-психологического воздействия. Рассматриваются технические и организационные меры защиты информации, направленные на сохранение конфиденциальности, целостности и доступности данных. Особое внимание уделяется применению криптографической защиты, защищенных каналов связи, а также мерам противодействия утечкам информации в современных условиях ведения боевых действий.

Ключевые слова: защита информации; информационная безопасность; радиоэлектронная борьба; криптографическая защита; каналы связи; военные информационные системы; утечка информации; кибербезопасность; средства защиты информации; информационные угрозы.

INFORMATION SECURITY DURING A SPECIAL MILITARY OPERATION

D.G. Muravitski, V.A. Fedorenko,

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. The paper considers the features of ensuring information security during a special military operation. The main threats to information systems and communication channels that arise during the active use of electronic warfare systems, intelligence tools and information-psychological operations are analyzed. Technical and organizational measures aimed at protecting information and maintaining the confidentiality, integrity and availability of data are considered. Particular attention is paid to the use of cryptographic protection, secure communication channels and measures to prevent information leakage in modern combat conditions.

Keywords: information security; electronic warfare; cryptographic protection; communication channels; military information systems; information leakage; cybersecurity; information protection technologies; electronic countermeasures; secure communication.

Введение

Современные вооруженные конфликты характеризуются активным применением информационных технологий и средств радиоэлектронной борьбы. В условиях специальной военной операции (СВО) защита информации становится ключевым фактором устойчивости управления войсками и сохранения боеспособности подразделений.

Информационные системы военного назначения обеспечивают передачу команд, управление вооружением и взаимодействие подразделений. Нарушение их функционирования может привести к потере управления, утечке секретных сведений и снижению эффективности действий войск.

В связи с этим особую актуальность приобретает внедрение комплексных мер защиты информации, направленных на предотвращение несанкционированного доступа, перехвата данных и воздействия средств РЭБ.

Основная часть

В ходе проведения специальной военной операции информационные системы и каналы связи подвергаются следующим основным угрозам: радиоэлектронное подавление подразделениями РЭБ; перехват и анализ радиопереговоров средствами радиоразведки; утечка информации через персональные устройства военнослужащих.

Широко применяются методы киберразведки, включая OSINT, социальную инженерию и анализ данных из социальных сетей. Противник осуществляет мониторинг мессенджеров, отслеживание геолокации и анализ метаданных фото- и видеоматериалов, что позволяет выявлять расположение и характер деятельности подразделений. Особую уязвимость представляет использование личных мобильных устройств, которые передают геоданные, подключаются к небезопасным сетям и могут содержать вредоносное ПО. Человеческий фактор становится причиной более 60% утечек информации.

Защиту информации обеспечивают подразделения связи, РЭБ и группы кибербезопасности. Подразделения связи развертывают защищенные каналы, РЭБ подавляет средства связи противника и защищает собственные каналы, а мобильные группы кибербезопасности ведут мониторинг цифровой активности и предотвращают утечки. Применяются криптографические методы: симметричные алгоритмы

(AES), асимметричные (RSA, ECC) и защищенные мессенджеры со сквозным шифрованием.

Технические меры включают использование экранирующих средств (мешки Фарадея) и технологию псевдослучайной перестройки рабочей частоты (ППРЧ), затрудняющую обнаружение и подавление сигналов. Организационные меры предусматривают инструктаж по информационной безопасности, запрет на использование личных устройств в зоне боевых действий и обучение личного состава основам цифровой гигиены, включая распознавание фишинга и методов социальной инженерии. Особое внимание уделяется контролю за использованием мобильных устройств и соблюдению правил защиты информации.

Комплексное применение технических, организационных и образовательных мер позволяет повысить устойчивость систем управления войсками и снизить вероятность утечки информации в условиях активного противодействия противника. Эффективность защиты информации напрямую зависит от согласованности действий подразделений связи, РЭБ и кибербезопасности, а также от уровня подготовки личного состава. Реализация комплексного подхода к защите информации обеспечивает устойчивость управления войсками и сохранение боеспособности подразделений при ведении современной войны.

Заключение

Таким образом, защита информации в условиях проведения специальной военной операции является важнейшим элементом обеспечения эффективности управления войсками. Активное применение противником средств радиоэлектронной борьбы и кибератак требует использования современных технологий информационной безопасности.

Повышение защищенности информационных систем достигается за счет применения криптографической защиты, защищенных каналов связи, распределенных систем передачи данных и строгих организационных мер безопасности. Реализация комплексного подхода к защите информации обеспечивает устойчивое функционирование систем управления и повышения эффективности действий подразделений в современных условиях боевых действий.

Список использованных источников

1. Манойло А. В. Фейки: траектория лжи. Информационный фронт специальной военной операции / А. В. Манойло, А. И. Петренко, Б. А. Рожин, К. С. Стригунов. – Москва : Горячая линия – Телеком, 2023. – 272 с.
2. Смирнов С. В. Криптографические методы защиты информации / С. В. Смирнов. – Санкт-Петербург : БХВ-Петербург, 2021. – 312 с.

3. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th ed. – London : Pearson, 2017. – 766 p.

References

1. Manoylo A.V., Petrenko A.I., Rozhin B.A., Strigunov K.S. Fakes: Trajectory of Lies. Information Front of the Special Military Operation. Moscow: Goryachaya liniya – Telekom, 2023. 272 p.

2. Smirnov S.V. Cryptographic Methods of Information Protection. St. Petersburg: BHV-Petersburg, 2021. 312 p. (in Russian)

3. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. London: Pearson, 2017. 766 p.

Сведения об авторах

Муравицкий Д.Г., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danikmuravitskiy@mail.ru

Федоренко В.А., начальник цикла кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.fedorenko@bsuir.by

Information about the authors

Muravitski D.G., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", danikmuravitskiy@mail.ru

Fedorenko V.A., Head of the cycle of the Department of Communications, Educational Institution "Belarusian State University of Informatics and Radioelectronics", v.fedorenko@bsuir.by

УДК 004.85:004.056.57

ВЛИЯНИЕ АРХИТЕКТУРЫ НЕЙРОННЫХ СЕТЕЙ НА ЭФФЕКТИВНОСТЬ ОБНАРУЖЕНИЯ ПРИЗНАКОВ ШИФРОВАНИЯ

В.Л. Мальцев, В.В. Возмитель, Е.В. Матяс

*Учреждение образования «Национальный детский технопарк», г. Минск,
Республика Беларусь*

Аннотация. В статье исследуется применение моделей глубокого обучения для идентификации зашифрованного содержимого. Рассмотрены полносвязные, сверточные сети, автоэнкодеры и трансформеры, проведен сравнительный анализ их эффективности при классификации байтовых последовательностей с использованием открытых наборов данных. Обоснована необходимость включения сжатых файлов в обучающую выборку для снижения ложных срабатываний в системах защиты информации. Полученные результаты демонстрируют преимущества редукции архитектур для повышения обобщающей способности моделей.

Ключевые слова: информационная безопасность; нейронные сети; шифрование; программы-вымогатели; машинное обучение; глубокое обучение; анализ энтропии; мониторинг файлов.

INFLUENCE OF NEURAL NETWORK ARCHITECTURE ON THE EFFICIENCY OF ENCRYPTION FEATURE DETECTION

V. Maltsau, V. Vozmitel, E. Matyas

Educational Institution "National Children's Technopark", Minsk, Republic of Belarus

Abstract. This article explores the application of deep learning models for identifying encrypted content, examining fully connected networks, convolutional networks, autoencoders, and transformers. A comparative analysis of the efficiency of byte sequence classification is conducted using open datasets. The necessity of including compressed files in the training set is substantiated to reduce the false positive rate in information security systems. The obtained results demonstrate the advantages of architecture reduction for improving model generalizability.

Keywords: information security; neural networks; encryption; ransomware; machine learning; deep learning; entropy analysis; file monitoring.

Введение

В условиях роста числа кибератак вопросы защиты пользовательских данных от программ-шифровальщиков приобретают критическое значение. Традиционные антивирусные решения, основанные на сигнатурном анализе или простых эвристиках (мониторинг энтропии), часто демонстрируют недостаточную точность при появлении новых угроз. Ключевым условием минимизации ущерба является обнаружение вредоносной активности на ранних стадиях, до завершения шифрования основного объема данных.

Основная часть

С целью выявления наиболее эффективных архитектур нейронных сетей для определения факта шифрования данных в процессе файловых операций был использован датасет NapierOne, содержащий более 300 тысяч образцов различных типов файлов. Ключевая проблема классификации заключается в схожести статистических характеристик зашифрованных и сжатых (архивных) данных. Для повышения надежности детектирования в обучающую выборку были включены файлы форматов .zip, .7z, .rar, а также другие документы с высокой плотностью упаковки данных.

В ходе работы были протестированы и проанализированы архитектуры:

1. *Полносвязные нейронные сети (FCNN)*: использовались как базовая модель. Входной вектор формировался на основе гистограммы частот байтов (256 значений). Несмотря на высокую скорость работы, FCNN ограничены в способности учитывать пространственные зависимости между байтами.

2. *Сверточные нейронные сети (CNN)*: входные данные представлялись

в виде одномерных векторов байтов. Применение фильтров позволило извлекать локальные признаки, характерные для заголовков различных файловых структур. Эксперименты показали, что CNN эффективнее справляются с отделением медиафайлов от зашифрованных блоков.

3. *Автоэнкодеры (AE)*: модель обучалась восстановлению «нормальных» (незашифрованных) последовательностей. Резкое увеличение функции потерь при реконструкции данных служило индикатором аномалии, указывающим на процесс шифрования.

4. *Трансформеры (Transformer)*: использование механизмов самовнимания позволило модели анализировать контекст всей последовательности данных. Это обеспечило наиболее точную идентификацию алгоритмов AES-256 в режиме реального времени.

Анализ интегрируется в систему мониторинга на базе Windows Minifilter. Драйвер перехватывает IRP-пакеты, извлекает буфер данных из операций записи и передает нейросетевому модулю. Тестирование показало, что комбинированный подход – анализ энтропии Шеннона совместно с предсказанием нейросети – снижает уровень ложных срабатываний до 0,5% при работе с офисными документами и архивами.

Для оценки влияния архитектурной емкости на обобщающую способность проведена серия экспериментов по редукции моделей. Исходная сверточная сеть (BaseFC) демонстрировала переобучение: разрыв точности между обучающей и тестовой выборками достигал 5%. Последовательное удаление слоев с усилением сжатия в узком месте привело к версии MiniFC, в которой дельта точности сократилась до 0,7%, а метрики F1-score и Precision улучшились на 4–5 % по сравнению с исходной конфигурацией. Дальнейшее сокращение параметров (NanoFC) вызвало недообучение.

Аналогичная закономерность выявлена для трансформеров. Исходная модель (BaseTR) после непродолжительного обучения (до 11 эпох) демонстрировала рост точности до 82%, затем впадала в катастрофическое переобучение. Версия MiniTR, полученная усечением выходных слоев и усилением сжатия, устранила этот дефект и превзошла исходную модель: точность достигла 88,1%, F1-score 0,887, коэффициент корреляции Мэтьюса – 0,771. Дальнейшая редукция (NanoTR) привела к росту полноты (Recall) до 99,3% за счет увеличения ложноположительных срабатываний, что допустимо в сценариях, где критически важно не пропустить ни одного зашифрованного файла. Результаты подтверждают, что избыточная параметрическая емкость вредна, а целенаправленная редукция архитектуры повышает обобщающую способность без дополнительных регуляризационных механизмов.

Заключение

Результаты подтверждают эффективность нейросетевых моделей для обнаружения ransomware-активности. Наилучший баланс точности и вычислительной эффективности достигается сверточными сетями и трансформерами при условии редукции архитектуры: удаление избыточных параметров устраняет переобучение и повышает обобщающую способность (версии MiniFC, MiniTR). Включение сжатых файлов в обучающую выборку снижает уровень ложных срабатываний. Реализация на базе Windows Minifilter позволяет блокировать подозрительные операции записи до необратимого изменения данных, что делает систему перспективным компонентом EDR-решений.

Список использованных источников

1. Гаттс, Дж. Глубокое обучение на Python / Дж. Гаттс. – СПб.: Питер, 2018. – 400 с.
2. Таненбаум, Э. Современные операционные системы / Э. Таненбаум, Х. Бос. – 4-е изд. – СПб.: Питер, 2015. – 1120 с.
3. Шай, Ш. Основы машинного обучения: от теории к алгоритмам / Ш. Шай, Ш. Бен-Давид; пер. с англ. – М.: ДМК Пресс, 2017. – 436 с.

References

1. Chollet, F. (2018) Deep Learning with Python. Saint Petersburg: Piter. (In Russian)
2. Tanenbaum, A., Bos, H. (2015) Modern Operating Systems. 4th ed. Saint Petersburg: Piter. (In Russian)
3. Shalev-Shwartz, S., Ben-David, S. (2017) Understanding Machine Learning: From Theory to Algorithms. Moscow: DMK Press. (In Russian)

Сведения об авторах

Мальцев В.Л. заведующий лабораторией «Информационная безопасность» учреждения образования «Национальный детский технопарк», viktor.maltsevlul@gmail.com.

Возмитель В.В. учащийся учреждения образования «Национальный детский технопарк», racfor4@gmail.com.

Матяс Е.В. учащийся учреждения образования «Национальный детский технопарк».

Information about the authors

Maltsau V. Head of the Information Security Laboratory, Educational Institution “National Children's Technopark”, viktor.maltsevlul@gmail.com.

Vozmitel V. student, Educational Institution “National Children's Technopark”, Minsk, Republic of Belarus, racfor4@gmail.com.

Matyas E. student, Educational Institution “National Children's Technopark”

УДК 004.62:004.056.5

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДОКУМЕНТООБОРОТА ЧЕРЕЗ ГИБРИДНЫЙ БЛОКЧЕЙН И ИЗОЛИРОВАННОЕ ИСПОЛНЕНИЕ КОДА

В.Л. Мальцев, С.А. Олексин, А.И. Самосюк

*Учреждение образования «Национальный детский технопарк»,
г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается система электронного документооборота на основе гибридного блокчейна и изолированного исполнения кода в виртуальной машине XVM. Неделимые токены (NFT) фиксируют хеши документов, разграничение ролей реализовано на уровне байт-кода. Детерминизм и криптографическая проверка целостности, дополненные изоляцией исполнения, обеспечивают пригодность системы для юридически значимого документооборота, гарантируя неизменяемость записей и повышая надежность хранения.

Ключевые слова: гибридный блокчейн; электронный документооборот; целостность данных; изолированное исполнение кода; виртуальная машина; песочница; неделимый токен; NFT; криптографическая подпись; детерминизм.

PROVIDING DOCUMENT FLOW VIA A HYBRID CABLE AND ISOLATED CODE EXECUTION

V. Maltsau, S. Aleksin, A. Samasiuk

*Educational Institution “National Children's Technopark”,
Minsk, Republic of Belarus*

Abstract. The paper considers an electronic document management system based on hybrid blockchain and isolated code execution in the XVM virtual machine. Non-fungible tokens (NFTs) record document hashes, role-based access control is implemented at the bytecode level. Determinism and cryptographic integrity verification, complemented by execution isolation, make the system suitable for legally significant document workflows, ensuring immutability of records and enhancing storage reliability.

Keywords: hybrid blockchain; electronic document management; data integrity; isolated code execution; virtual machine; sandbox; non-fungible token; NFT; digital signature; determinism.

Введение

Электронный документооборот и количество подписей с помощью ЭЦП неуклонно растут, вытесняя бумагу. Однако остается открытым вопрос о достаточности существующих инструментов для обеспечения надежности и безопасности такого перехода. Большой популярностью пользуются централизованные системы провайдеров, однако они имеют ряд недостатков. Один из главных – отсутствие гарантии неизменяемости действий и недостаточно гибкая система разграничения прав доступа.

Основная часть

Предлагаемое решение использует гибридный блокчейн, сочетающий неизменяемость данных, криптографическую защиту и тонкое управление доступом. Участники разделены на уровни прав (типы кошельков A–D). Цифровым представлением документов служат неделимые токены (NFT), в метаданных которых хранятся хеш документа, адрес владельца, срок действия и иные сведения. NFT не является подлинником, но доказывает существование документа и историю операций; после истечения срока или отмены токен сжигается, а записи о всех операциях навсегда сохраняются в блокчейне.

Ядро системы – виртуальная машина XVM (eXtended Virtual Machine) с изолированным исполнением кода. XVM построена по стековому принципу, включает стек данных, стек вызовов, глобальную память и динамическую кучу. Детерминизм (одинаковый результат на любом узле) достигается фиксированным набором из 63 опкодов и отсутствием недетерминированных системных вызовов. Изоляция реализована через классическую «песочницу»: код не может напрямую обращаться к файловой системе, сети или памяти других процессов; взаимодействие с внешней средой возможно только через контролируемые системные вызовы. Среда исполнения отслеживает потребление ресурсов, прерывая выполнение при превышении лимита инструкций, что предотвращает DoS-атаки.

Проверка прав доступа встроена в интерпретатор байт-кода: роль пользователя хранится в структуре кошелька, и при попытке привилегированного действия анализ роли выполняется до обработки остальных инструкций. Криптографические операции (SHA-512, генерация ключей Ed25519) реализованы нативными опкодами, передающими данные в высокопроизводительные модули хост-системы, что сохраняет атомарность и обеспечивает высокую скорость обработки транзакций.

Процесс работы с документами строится на неизменяемых записях в реестре. При выпуске документа формируется транзакция создания NFT, фиксирующая 512-битный хеш файла, идентификатор владельца, временную метку и статус. Транзакция подписывается закрытым ключом эмитента и упаковывается в блок. Передача прав инициируется текущим владельцем: в транзакции указываются идентификатор NFT и адрес нового владельца, XVM проверяет право и обновляет запись, сохраняя полную

хронологию. Даже при «сжигании» документа все предыдущие записи остаются нетронутыми.

Такая архитектура меняет модель доверия: администратор не может скрыто изменить записи – попытка модификации нарушает хеш-связку блоков, что обнаруживается функцией периодической проверки целостности. Это обеспечивает невозможность отказа от авторства и доказуемую целостность истории, что критически важно для юридически значимых документов.

Блокчейн развернут как сеть взаимодействующих серверов с дублированием данных. Любое действие подтверждается подписью транзакции, буферный сервер проверяет подпись и передает запрос основному серверу. Основной набор команд включает создание, передачу и уничтожение NFT, управление кошельками, информационные запросы. Для расширения функционала предусмотрена возможность создания модулей на языке xLang (C-подобный язык со встроенными криптофункциями), работающих внутри песочницы.

Предлагаемая система сочетает высокую безопасность, прозрачность и гибкость, что делает ее перспективным решением для задач, требующих гарантированной достоверности данных.

Заключение

Предложенная архитектура электронного документооборота на основе гибридного блокчейна и изолированного исполнения кода обеспечивает криптографическую подтверждаемость операций, неизменяемость данных и защиту от несанкционированной модификации, что делает ее пригодной для юридически значимого документооборота. Предложенная архитектура масштабируема и адаптируема за счет возможности расширения функционала модулями на языке xLang, что открывает перспективы для внедрения системы в организациях с высокими требованиями к достоверности и прозрачности документооборота.

Список использованных источников

1. Конорев, Н., С. Мазуров, С. Перспективы применения технологии блокчейн в Республике Беларусь. – Минск: жур. «Банкаўскі веснік», разд. Цифровые технологии – 2000-2025. – с. 66-71.
2. Косба А., Миллер А., Ши Э., Вэнь З., Папаманту К. Hawk: модель криптографии с сохранением конфиденциальности для блокчейна и смарт-контрактов // 2016 IEEE Symposium on Security and Privacy (SP). – 2016. – С. 839–858.

References

1. Konorev N., Mazurov S. Prospects for the application of home lighting technologies in the Republic of Belarus // Bankauski vesnik. – 2025. – P. 66–71. (in Russian).
2. Kosba A., Miller A., Shi E., Wen Z., Papamantou C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts // 2016 IEEE Symposium on Security and Privacy (SP). – 2016. – P. 839–858.

Сведения об авторах

Мальцев В.Л. – заведующий лабораторией «Информационная безопасность» учреждения образования «Национальный детский технопарк», viktor.maltsevlul@gmail.com.

Олексин С.А. – учащийся учреждения образования «Национальный детский технопарк», г. Минск, Республика Беларусь, e-mail: simonoleksin@gmail.com.

Самосюк А.И. – учащийся учреждения образования «Национальный детский технопарк», г. Минск, Республика Беларусь, e-mail: sasha20ahsas@gmail.com.

Information about the authors

Maltsau V. – Head of the Information Security Laboratory, Educational Institution “National Children's Technopark”, viktor.maltsevlul@gmail.com.

Aleksin S. – student Educational Institution “National Children's Technopark”, simonoleksin@gmail.com.

Samasiuk A. – student, Educational Institution “National Children's Technopark”, Sasha20ahsas@gmail.com.

УДК 004.056.53

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПОДЛИННОСТИ RFID-МЕТОК

А.О.Ворожцов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Метки типа RFID, в силу передачи данных по радиоканалу, уязвимы к атакам вида relay и replay. Для предотвращения использования нарушителем перехваченных данных предлагается дополнительный метод определения подлинности карты. Антенна карты меняется на печатную щелевую, с о случайным расположением щелей, формирующим уникальный паттерн плотности магнитного поля.

Ключевые слова: RFID, HF, UHF, антенна, диаграмма направленности, плотность магнитного поля, Matlab, Relay-атака, Replay-атака, щелевая антенна.

METHOD OF DEFINING THE RFID TAGS IDENTITY

A.O. Voroztsov

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. RFID tags, due to usage of radio channel to transmit data, are vulnerable to Relay and Replay types of attacks. To prevent intruder from using captured data, an additional

identification method is proposed. Antenna is changed to slot PCB antenna with random slot positioning, that forms unique pattern of magnetic field density.

Keywords: RFID, HF, UHF, antenna design, radiation pattern, magnetic field density, Matlab, Relay-attack, Replay-attack, slot antenna.

Введение

В настоящее время довольно активно используются бесконтактные идентификаторы типа RFID. Данные идентификаторы имеют широкое применение в областях, где требуется быстрое получение информации с метки. Чаще всего применяются программные методы, вида шифрования, реализованного на метке, передачи ранее записанных случайных чисел, замеры времени для предотвращения Relay-атак. В данной работе предлагается добавление дополнительного физического идентификатора подлинности, который будет более дорогим и трудоемким для подделки. Основной фокус идет на метки диапазона UHF—856-868 и 902-928 МГц для Европы и США соответственно, но может быть применен и к меткам диапазона HF—13,56 МГц.

Основная часть

UHF и HF идентификаторы применяются в большом количестве областей, как то СКУД, маркировка товаров, общественный транспорт, логистика и многое другое. UHF метки часто применяются для маркировки товаров, в силу хорошей электромагнитной совместимости и возможности сделать антенну малого размера. В силу применения радиоэфира для передачи данных, существует большое количество решений для реализации различных атак, как специализированных, типа ProxMark3, так и универсальных, типа HackRF. Два основных вида атак, Relay и Replay, имеют одно общее ограничение: сигнал от метки передается или генерируется устройством нарушителя в силу того, что метка находится вне зоны действия терминала. Программные методы защиты фокусируются на передаче информации, которую нарушитель может перехватить, но не сможет применить повторно, как-то ранее переданное случайное число или ключ сессии. Данные средства защиты частично обходятся методами атак по побочным каналам или уязвимостями, заложенными производителями.

Предлагается следующее средство защиты меток: антенна метки меняется на печатную щелевую антенну со случайным расположением и размерами щелей, получаемых травлением или фрезеровкой, за счет чего каждая метка будет иметь уникальную диаграмму напряженности магнитного поля. Так как щель функционирует подобно диполю, изменением их размеров и местонахождения на покрытии возможно получить значительное количество различных паттернов, с разной

энтропией, градиентом и коэффициентом отражения. В силу большей рабочей зоны UHF меток, позволяющей использовать для идентификации коэффициент отражения, и меньшей длины волны, увеличивающей влияние строения антенны на диаграмму направленности, рекомендуется использовать идентификаторы UHF диапазона.

В силу работы в ближней зоне (< 5 см) предполагается измерение плотности магнитного поля, так как диаграмма направленности имеет значимую роль лишь в дальней зоне. Терминал оснащается антенной решеткой, позволяющей измерить плотность магнитного поля в разных точках пространства и вспомогательным контроллером, рассчитывающим градиент и коэффициент отражения для несущей частоты. Данные значения передаются основному контроллеру, для ускорения процесса возможно привязать данные значения к ключу шифрования некоторой функцией, уникальной для каждой метки.

$$G_u = \frac{1}{M} \sum_{i=1}^M \frac{|U_i - U_j|}{d_{ij}}, \quad (1)$$

где G_u – градиент; M – число элементов; U – напряжение; d_{ij} – расстояние между элементами

$$|Ku| = \frac{U_{\text{отп}}/U_{\text{вых}}}{e^{j\Delta\phi}}, \quad (2)$$

где $|Ku|$ – модуль коэффициента отражения; $U_{\text{отп}}$ – принятое U несущей (с поправкой на АЧХ антенны и затухание); $U_{\text{вых}}$ – U несущей на выходе терминала; $e^{j\Delta\phi}$ – волновой коэффициент по $\Delta\phi$

$$\Delta\phi = -f \frac{d\phi}{df}, \quad (3)$$

где ϕ – мгновенная фаза; f – несущая частота.

Расчеты проводились в САПР Matlab, на базе которого возможно создать приложение, рассчитывающее некоторое количество чертежей антенн с достаточной уникальностью для однозначной идентификации метки.

Для обхода данной методики защиты помимо длительного контакта с меткой, что уже отпугнет большую часть нарушителей, потребуется наличие оборудования, способного измерить характеристики антенны, ПО для расчета антенны по данным характеристикам и оборудования для создания идентичной антенны. В силу этого, для проведения атаки нарушитель должен иметь значительный уровень подготовки и материально-технического обеспечения.

Заключение

Полученный метод позволяет более определять подлинность RFID меток на физическом уровне, без изменения протокола, контроллеров метки и терминала, требуя лишь изменения антенны метки, антенны терминала и установки вспомогательного контроллера. Данный метод применим к любым картам диапазонов HF и UHF, обеспечивая бюджетную и эффективную защиту.

Список использованных источников

1. В. В. Муравьев, А. А. Тамело, Д. Ф. Молодкин, Д. Б. Владимиров (2010) Расчет и проектирование антенн и устройств СВЧ. – Минск, БГУИР.
2. Таненбаум А. Эволюция безопасности RFID//IEEE Security & privacy. – 2006. – Т.4, № 2. – С. 62-69.

References

1. V. Muravyev, A. A. Tamelo, D. F. Molodkin, D. B. Vladimirov (2010) Calculation and production of antennas and microwave devices. – Minsk, BSUIR.
2. Tanenbaum A. The evolution of RFID security//IEEE Security & privacy. – 2006. – Vol.4, No. 2. – P. 62-69.

Сведения об авторе

Ворожцов А.О. Студент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», amdreyvorog2007@gmail.com.

Information about the author

Varazhtsou A., student of Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics" amdreyvorog2007@gmail.com.

УДК 621.39

ЗАЩИЩЕННАЯ СИСТЕМА РАДИОУПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ И КРИПТОГРАФИЧЕСКИМ ШИФРОВАНИЕМ

¹Я.А. Мойсюк-Дранько, ²И.А. Дубовик

¹Учреждение образования «Национальный детский технопарк»,
г. Минск, Республика Беларусь

²Учреждение образования «Военная академия Республики Беларусь»,
г. Минск, Республика Беларусь

Аннотация. В статье рассматривается комплексный подход к обеспечению защищенности канала связи с беспилотными летательными аппаратами в условиях радиоэлектронного противодействия. Проведен анализ криптографических алгоритмов, обоснован выбор AES-256 для защиты командно-телеметрической информации. Представлена реализация метода псевдослучайной перестройки радиочастоты с использованием перемешанного конгруэнтного генератора. Разработанное решение обеспечивает высокий уровень криптографической стойкости и помехоустойчивости канала связи.

Ключевые слова: беспилотный летательный аппарат; радиосвязь; криптографическая защита; AES; псевдослучайная перестройка рабочей частоты; радиоэлектронное противодействие; перемешанный конгруэнтный генератор; помехозащищенность; перехват команд; телеметрия.

A SECURE RADIO CONTROL SYSTEM FOR AN UNMANNED AERIAL VEHICLE WITH FREQUENCY-HOPPING SPREAD SPECTRUM AND CRYPTOGRAPHIC ENCRYPTION

¹Y.A. Moisiuk-Dranko, ²I.A. Dubovik

¹*Educational Institution "National Children's Technopark",
Minsk, Republic of Belarus*

²*Educational Institution "Military academy the Republic of Belarus",
Minsk, Republic of Belarus*

Abstract. This article examines a comprehensive approach to ensuring the security of communications with unmanned aerial vehicles (UAV) in the face of electronic countermeasures. An analysis of cryptographic algorithms is conducted, substantiating the choice of AES-256 for protecting command and telemetry information. An implementation of a frequency hopping spread spectrum method using a permuted congruential generator is presented. The developed solution ensures a high level of cryptographic security and noise immunity for the communication channel.

Keywords: unmanned aerial vehicle; radio communication; cryptographic protection; AES; frequency hopping spread spectrum; electronic countermeasures; permuted congruential generator, interference immunity; command interception; telemetry.

Введение

Эффективность применения беспилотных летательных аппаратов (далее - БЛА) напрямую зависит от защищенности канала связи. В условиях интенсивного радиоэлектронного противодействия существующие системы управления БЛА сталкиваются с угрозами перехвата команд, постановки помех и захвата управления.

Основная часть

Для обеспечения конфиденциальности и целостности передаваемых данных был проведен сравнительный анализ алгоритмов симметричного шифрования: AES, 3DES и RC4.

Алгоритм AES-256 демонстрирует оптимальное сочетание криптографической стойкости и производительности. При использовании 256-битного ключа обеспечивается стойкость на уровне 2^{256} комбинаций, что делает атаки полным перебором практически невозможными. Высокая скорость шифрования критически важна для систем реального времени.

Алгоритм 3DES, представляющий собой трехкратное применение алгоритма DES, не гарантирует достаточную защиту БЛА.

Потоковый шифр RC4 был исключен вследствие выявленных критических уязвимостей в генерации ключевого потока и возможности статистических атак при определенных условиях использования.

На основе проведенного анализа выбран алгоритм AES-256 как оптимальное решение для защиты команд и телеметрии БЛА.

Для защиты от радиоэлектронного противодействия применен метод псевдослучайного переключения рабочей частоты (далее – ППРЧ), основанный на быстром переключении несущей частоты передатчика по псевдослучайному закону, известному обеим сторонам канала связи. Метод ППРЧ обладает рядом существенных преимуществ. Обеспечивается скрытность передачи: быстрое переключение частот создает сигнал, неразличимый для средств радиоразведки противника, что значительно затрудняет обнаружение и идентификацию канала связи. Достигается высокая помехозащищенность: для эффективного подавления сигнала с ППРЧ противнику необходимо создавать помеху в широкой рабочей полосе частот, что требует значительно большей мощности по сравнению с постановкой помех на фиксированной частоте. Система демонстрирует устойчивость к узкополосным помехам: даже при наличии мощной помехи на отдельных частотах общая пропускная способность канала снижается пропорционально отношению подавленных частот к общему числу используемых каналов.

Критически важным элементом системы ППРЧ является генератор псевдослучайных чисел, определяющий последовательность смены рабочих частот. Для генерации последовательности выбран перемешанный конгруэнтный генератор (далее - PCG). PCG сочетает преимущества линейных конгруэнтных генераторов с дополнительным этапом перемешивания выходных значений.

PCG обеспечивает минимальные корреляционные паттерны, что критически важно для предотвращения предсказания последовательности переключения частот противником. Высокая производительность генератора позволяет реализовать частоту переключения до нескольких тысяч скачков в секунду без создания значительной вычислительной нагрузки на микроконтроллер системы управления БЛА.

Синхронизация передающей и приемной сторон осуществляется путем использования общего начального значения (seed) для

PCG-генератора, передаваемого по защищенному каналу на этапе инициализации системы. Данный подход позволяет обеим сторонам независимо генерировать идентичную последовательность.

Заключение

Разработано комплексное решение по защите канала связи с БЛА, сочетающее криптографическую защиту AES-256 и радиочастотную защиту методом ППРЧ с PCG-генератором. Многоуровневая архитектура обеспечивает высокую стойкость к радиоэлектронному противодействию, требуя от противника одновременного преодоления криптографической и радиочастотной защиты.

Список использованных источников

1. Singh G., Supriya A. (2013) A Study of Encryption Algorithms for Information Security. *International Journal of Computer Applications*. 67 (19), 33-38.
2. O'Neill M. (2014) PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation. *Technical Report HMC-CS-2014-0905, Harvey Mudd College*.
3. Daemen J., Rijmen V. (2002) *The Design of Rijndael: AES — The Advanced Encryption Standard*. Germany, Springer-Verlag.
4. Torrieri D. (2015) *Principles of Spread-Spectrum Communication Systems*. Germany, Springer.

References

1. Singh G., Supriya A. (2013) A Study of Encryption Algorithms for Information Security. *International Journal of Computer Applications*. 67 (19), 33-38.
2. O'Neill M. (2014) PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation. *Technical Report HMC-CS-2014-0905, Harvey Mudd College*.
3. Daemen J., Rijmen V. (2002) *The Design of Rijndael: AES — The Advanced Encryption Standard*. Germany, Springer-Verlag.
4. Torrieri D. (2015) *Principles of Spread-Spectrum Communication Systems*. Germany, Springer.

Сведения об авторах

Мойсюк-Дранько Я.А., учащийся, учреждение образования «Национальный детский технопарк», jajaroslove@gmail.com.

Дубовик И.А., канд. техн. наук, доц., доц. каф. тактики и вооружения радиотехнических войск факультета противовоздушной обороны, учреждение образования «Военная академия Республики Беларусь», dubaiilia94@gmail.com.

Information about the authors

Moisiuk-Dranko Y.A., student, educational institution “National children’s technopark”, jajaroslove@gmail.com.

Dubovik I.A., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Tactics and Armament of Radiotechnical Troops of the Faculty of Air Defense, educational institution “Military academy the Republic of Belarus”, dubaiilia94@gmail.com.

УДК 004.056

ИНСТРУМЕНТ ДЛЯ OSINT-РАЗВЕДКИ И РЕАЛИЗАЦИИ ТЕХНИКИ MITRE ATT&CK T1593

И.А. Войткус, Е.С. Белоусова

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматривается автоматизация сбора данных киберразведки по технике MITRE ATT&CK T1593. Разработан инструмент для OSINT-разведки на базе low-code платформы n8n, включающий три процесса: поиск скрытых документов, анализ репозиторий и визуальную разведку. Апробация разработанного инструмента была проведена на ресурсах БГУИР и подтвердила высокую скорость профилирования цифрового следа и масштабируемость решения.

Ключевые слова: разведка по открытым источникам; киберразведка; тактика T1593; автоматизированный сбор данных; биометрическая верификация; сбор информации; агрегация данных

AUTOMATION OF OSINT INTELLIGENCE BASED ON MITRE ATT&CK T1593 TECHNIQUE

I.A. Voitkus, E.S. Belousova

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article discusses the automation of cyber intelligence data collection using MITRE ATT&CK T1593 technology. A tool based on the n8n low-code platform has been developed, which includes three processes: search for hidden documents, repository analysis, and visual intelligence. Testing on the BSUIR resources confirmed the high speed of digital footprint profiling and scalability of the solution

Keywords: open-source intelligence; cyber intelligence; T1593 tactics; automated data collection; biometric verification; information collection; data aggregation

Введение

Киберразведка – начальный и ключевой этап реализации киберугроз в рамках модели «Cyber Kill Chain» [1]. Множественные массивы корпоративных и персональных данных, опубликованные на официальных ресурсах и сторонних платформах, формируют «цифровой след»

Основная часть

343

Полученные данные содержат поля имени, фамилии и отчества, для корректной работы поисковых алгоритмов в конвейер была добавлена нода трансформации данных, формирующая единый унифицированный идентификатор. Далее инструмент на втором этапе инициирует разделение данных на три процесса.

Первый процесс осуществляет поиск скрытых документов на поддоменах университета. Система автоматически генерирует запрос через легитимный API-шлюз для предотвращения блокировок, возвращая готовый массив ссылок на найденные файлы. Запрос возвращает готовый список прямых ссылок на найденных документах.

Второй процесс выявляет у субъекта публичные репозитории кода, выступающие потенциальным источником утечек информации. Возникшая при настройке узлов проблема потери контекста была успешно решена архитектурно – путем принудительного проброса переменных через всю цепочку конвейера. На выходе сохраняются отфильтрованные ссылки на профили выявленных субъектов.

Третий процесс выполняет комплексный анализ визуального следа. Инструмент Photon позволил собрать ссылки на социальные сети и доменные адреса, а также конвейер инициирует HTTP-запросы на скачивание графических файлов, формируя оффлайн-базу данных. Консольная утилита ExifTool анализирует структуру каждого файла в поиске скрытых цифровых следов. Локальная верификация с помощью библиотеки машинного зрения DeepFace, сравнивает найденные лица с эталонным фото, гарантируя конфиденциальность вычислений.

Заключение

На платформе n8n разработан и протестирован инструмент для OSINT-разведки. Инструмент позволил собрать базу данных субъектов и провести дальнейшие поиски по ней. Предложенная архитектура обладает высокой гибкостью и может быть масштабирована путем интеграции новых инструментов.

Список использованных источников

1. Блэр, Р. Согласование операций безопасности с фреймворком MITRE ATT&CK / Р. Блэр. – Бирмингем: Packt Publishing, 2022. – 268 с. – ISBN 978-1804616697.
2. Озкая, Э. Практическая киберразведка: сбор, обработка и анализ мотивов, целей и атак злоумышленников / Э. Озкая. – Нью-Дели: BPB Publications, 2022. – 452 с. – ISBN 978-9355510372.

References

1. Blair, R. Aligning Security Operations with the MITRE ATT&CK Framework / R. Blair. – Birmingham: Packt Publishing, 2022. – 268 p. – ISBN 978-1804616697.

2. Ozkaya, E. Practical Cyber Threat Intelligence: Gather, process, and analyze threat actor motives, targets, and attacks / E. Ozkaya. – New Delhi: BPB Publications, 2022. – 452 p. – ISBN 978-9355510372.

Сведения об авторах

Войткус И.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», voitkusvoitkus@gmail.com.

Белоусова Е.С., канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Voitkus I.A., student of Information Security Faculty, Belarusian State University of Information Technology and Radio Electronics, voitkusvoitkus@gmail.com.

Belousova E.S., PhD, Associate Professor, Information Security Department, Belarusian State University of Informatics and Radioelectronics, belousova@bsuir.by.

УДК 621.382

ОБУЧАЮЩИЙ ЭКСПЕРИМЕНТ КАК ОСНОВА ПОЛУЧЕНИЯ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ НАДЕЖНОСТИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

И.В. Русак

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Для получения модели индивидуального прогнозирования класса надежности полупроводниковых приборов для заданной наработки по значениям их информативных параметров в начальный момент времени необходимо иметь результаты обучающего эксперимента. Для проведения обучающего эксперимента следует знать информативные параметры полупроводниковых приборов. В качестве приборов были выбраны полевые транзисторы большой мощности типа КП744А. Измерение электрических параметров, предполагаемых на информативность, испытание транзисторов на надежность и дальнейшее определение корреляционной связи параметров с номером класса надежности приборов на момент окончания испытаний, позволили определить три наиболее информативных параметра и сформировать таблицу результатов обучающего эксперимента, используемого для получения модели прогнозирования класса надежности экземпляров для заданной наработки.

Ключевые слова: информативные параметры; полевые транзисторы; класс надежности; индивидуальное прогнозирование; корреляционный анализ.

TEACHING EXPERIMENT AS THE BASIS FOR OBTAINING MODELS FOR PREDICTING THE RELIABILITY OF SEMICONDUCTOR DEVICES

I.V. Rusak

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. To obtain a model for individually predicting the reliability class of semiconductor devices for a given service life based on the values of their informative parameters at the initial time, it is necessary to have the results of a training experiment. To conduct the training experiment, it is necessary to know the informative parameters of the semiconductor devices. High-power field-effect transistors of the KP744A type were selected as the devices. Measuring the electrical parameters expected to be informative, testing the transistors for reliability, and then determining the correlation between the parameters and the device reliability class number at the end of the tests allowed us to identify the three most informative parameters and generate a table of the training experiment results used to obtain a model for predicting the reliability class of samples for a given service life.

Keywords: informative parameters; field-effect transistors; reliability class; individual forecasting; correlation analysis.

Введение

Одним из способов обеспечения высоких показателей безотказности электронной аппаратуры является установка в нее полупроводниковых приборов повышенного уровня надежности. Перед тем как это сделать необходимо выполнить отбор экземпляров (единиц приборов) повышенного уровня надежности. Эффективным способом решения данной задачи является индивидуальное прогнозирование класса надежности экземпляров для заданной наработки, используя информативные параметры полупроводниковых приборов в начальный момент времени. Информативные параметры каждого экземпляра измеряются в начальный момент времени и по их значениям может прогнозироваться класс работоспособности (надежности) данного экземпляра для заданной наработки: K_1 – класс надежных, K_2 – класс потенциально ненадежных экземпляров [1].

Для поиска информативных параметров необходимо в начальный момент времени у каждого экземпляра выборки полупроводниковых приборов интересующего типа измерить электрические параметры, которые гипотетически могут оказаться информативными. Выборку приборов называют обучающей. Ее объем должен составлять примерно 50...200 экземпляров. Перед проведением измерений экземпляры выборки должны быть пронумерованы. Далее выполняют испытания обучающей выборки на надежность, используя обычно ускоренные форсированные испытания, эквивалентные с точки зрения работоспособности интересующей заданной наработке в обычных нормальных условиях работы. После окончания испытаний уточняется класс каждого экземпляра с точки зрения его работоспособности (надежности). Информативность электрических параметров может определяться методом корреляционного анализа [2].

Основная часть

В ходе выполнения работы решалась задача поиска информативных параметров и проведения обучающего эксперимента для полевых транзисторов типа КП744А. Объем обучающей выборки составлял 187 экземпляров. В качестве измеряемых были выбраны электрические параметры, как нормируемые в технической документации, так и специфические параметры.

При решении задач индивидуального прогнозирования класса надежности изделий электронной техники обычно используют 3–5 информативных параметра. Для принятия решения о выборе параметров, используемых в качестве информативных, были определены коэффициенты парной корреляции электрических параметров с номером класса надежности экземпляров (1 или 2). Для определения коэффициентов корреляции использовался инструмент «Корреляция» пакета «Анализ данных» компьютерной программы Microsoft Excel. В таблице приведен фрагмент полученной корреляционной матрицы, в которую включены три наиболее информативных параметра.

Корреляционная матрица параметров (транзисторы типа КП744А)
Correlation matrix of parameters (transistors type KP744A)

Электрический параметр, класс надежности	$U_{\text{зи.пор}}$	$C_{\text{зс}}$	$C_{\text{зи}}$	S
$U_{\text{зи.пор}}$	1	–	–	–
$C_{\text{зс}}$	-0,729	1	–	–
$C_{\text{зи}}$	-0,521	0,577	1	–
S – номер класса надежности для заданной наработки $t = 16100$ ч	-0,635	0,603	0,416	1

Пояснение электрических параметров, используемых в качестве информативных для заданной наработки $t = 16100$ ч:

$U_{\text{зи. пор}}$ – пороговое напряжение затвор–исток;

$C_{\text{зс}}$ – емкость затвор–сток;

$C_{\text{зи}}$ – емкость затвор–исток.

Заключение

Для проведения обучающего эксперимента и поиска информативных параметров, используемых для прогнозирования класса надежности полевых транзисторов типа КП744А, были измерены электрические параметры, предполагаемые на информативность, у каждого экземпляра обучающей выборки. В качестве критерия информативности

рассматривался модуль коэффициента корреляции между значениями электрического параметра в начальный момент времени и номером класса надежности экземпляров обучающей выборки на момент окончания ускоренных испытаний транзисторов. Выполненные исследования позволили определить три наиболее информативных параметра и сформировать таблицу результатов обучающего эксперимента, используемого для получения модели прогнозирования класса надежности для заданной наработки однотипных экземпляров, не принимавших участия в испытаниях.

Список использованных источников

1. Боровиков С.М. (2013) *Статистическое прогнозирование для отбраковки потенциально ненадежных изделий электронной техники*. Москва, Издательство «Новое знание».
2. Боровиков С.М. (1998) *Теоретические основы конструирования, технологии и надежности*. Минск, Издательство «ДизайнПРО».

References

1. Borovikov S.M. (2013) *Statistical Forecasting for Rejection of Potentially Unreliable Elec-tronic Products*. Moscow, New Knowledge Publishing House.
2. Borovikov S.M. (1998) *Theoretical Foundations of Design, Technology and Reliability*. Minsk. DesignPRO Publishing House.

Сведения об авторах

Русак И.В., магистрант кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», iliaru756@gmail.com.

Information about the authors

Rusak I., Postgraduate of the Department of Information and Computer System Design, Educational Institution "Belarusian State University of Informatics and Radioelectronics", iliaru756@gmail.com

УДК 342.723

МЕЖДУНАРОДНЫЙ ОПЫТ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Г.А.Пухир, Р.В.Шерышев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе проводится сравнительный анализ подходов к регулированию деятельности в сфере защиты информации в различных юрисдикциях. Рассматриваются белорусская и российская модели, основанные на государственном

регулировании посредством лицензирования технической и криптографической защиты информации, а также подходы Казахстана и Китая, демонстрирующие некоторые схожие черты. Показано, что в США и ЕС представлены иные системы, где отсутствует единый принцип лицензирования деятельности по технической и криптографической защите информации, а регулирование строится на отраслевых требованиях, сертификации и стандартизации. Делается вывод о двух основных моделях регулирования: разрешительной и контрольно-надзорной.

Ключевые слова: лицензирование; защита информации; кибербезопасность; модели регулирования; государственный контроль; разрешительный порядок; сертификация; стандарты; надзорные органы; информационная безопасность.

INTERNATIONAL EXPERIENCE IN STATE REGULATION OF INFORMATION PROTECTION

H.A. Pukhir, R.V. Sheryshev

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The paper provides a comparative analysis of approaches to regulating information security activities in various jurisdictions. The article considers the Belarusian and Russian models based on government regulation through licensing of technical and cryptographic information protection, as well as the approaches of Kazakhstan and China, which demonstrate some similar features. It is shown different systems in the United States and the EU, where there is no unified licensing of technical and cryptographic information protection, and regulation is based on industry requirements, certification and standardization. It is concluded that there are two main models of regulation: permissive and supervisory.

Keywords: licensing; information protection; cybersecurity; regulatory models; government control; permitting procedure; certification; standards; supervisory authorities; information security.

Введение

Информация в современном мире стала стратегическим ресурсом, требующим надежной защиты. В условиях трансграничного информационного обмена особую значимость приобретает изучение международного опыта регулирования этой сферы. Анализ существующих подходов необходим для понимания того, как минимизировать риски, связанные с двойственным характером знаний в области защиты информации, и выработки эффективных механизмов противодействия современным угрозам.

Основная часть

В Республике Беларусь деятельность в сфере защиты информации осуществляется на основе лицензирования, согласно Закону Республики Беларусь от 14 октября 2022 г. № 213-З «О лицензировании» и Указу Президента Республики Беларусь от 16 февраля 2012 г. №71 «О порядке

лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)».

Лицензирование деятельности по технической и (или) криптографической защите информации, включая применение электронной цифровой подписи, осуществляет Оперативно-аналитический центр при Президенте Республики Беларусь, а в части средств криптографической защиты государственных секретов и специфических средств – Комитет государственной безопасности.

Лицензирование деятельности в сфере защиты информации в Российской Федерации регулируется Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», а также Постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» и Постановлением Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю (ФСТЭК). Лицензирование деятельности по защите информации, связанной с государственной тайной, а также выявлением электронных устройств для негласного получения информации осуществляет ФСБ России.

Среди других стран СНГ, в Казахстане действует строгая система лицензирования деятельности по защите информации через Комитет национальной безопасности Республики Казахстан (КНБ РК): требуется предварительное разрешение для работы со средствами криптографической защиты информации.

Если рассмотреть азиатский регион, например, в Китае отсутствует единая государственная лицензия на деятельность по защите информации, однако регулирование осуществляется через жесткие законы о кибербезопасности (Закон КНР о сетевой безопасности 2017 г. с поправками 2026 г., Закон о безопасности данных и Закон о защите персональной информации) [1]. Эти акты обязывают компании, особенно операторов критической информационной инфраструктуры, внедрять системы многоуровневой защиты (MLPS), сертифицировать средства криптографии, хранить логи и отчитываться перед контролирующими органами, такими как Администрация по киберпространству Китая и Государственное управление по регулированию рынка.

В Европейском Союзе (ЕС) отсутствует единое обязательное государственное лицензирование на деятельность по защите информации в целом. Регулирование осуществляется через сертификацию, стандарты и надзор со стороны национальных органов с акцентом на соблюдение

регламента GDPR, директивы NIS2 и национальных законов. Деятельность по защите информации также регламентируется международными стандартами серии ISO/IEC 27000:2022 [2].

В отличие от многих других стран, в США сформировалась принципиально иная, децентрализованная модель регулирования. В Соединенных Штатах отсутствует понятие единой федеральной лицензии на деятельность в сфере защиты информации. Вместо этого, требования к компаниям и специалистам определяются отраслевой принадлежностью организации, типом обрабатываемых данных и характером взаимодействия с государством.

Заключение

В мире сложились принципиально разные подходы к регулированию деятельности в сфере защиты информации. В США и ЕС отсутствует единое лицензирование такой деятельности. Западные регуляторы контролируют результаты и процессы, но не устанавливают разрешительного порядка допуска к профессии. Беларусь, Россия и некоторые другие страны пошли иным, уникальным путем. Государство выполняет функцию уполномоченного регулятора, осуществляющего предварительный контроль и выдачу разрешений на осуществление деятельности по защите информации.

Список использованных источников

1. Ромашкина Н., Задремайлова В. Эволюция политики КНР в области информационной безопасности // Пути к миру и безопасности. 2020, №1(58). – С.122-138.
2. Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций: образование, наука, новая экономика. 2020, Т. 15, № 2. – С. 105-124.

References

1. Romashkina N., Zadremailova V. The Evolution of China's Information Security Policy // Paths to Peace and Security, No. 1(58), 2020. – P. 122-138.
2. A. Verhelst, J. Wouters Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives // International organisations research journal. Vol. 15. No 2 (2020) – P. 105-124.

Сведения об авторах

Пухир Г.А., старший преподаватель кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», puhir@bsuir.by.

Шерышев Р.В., студент гр. 561401 факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», romasheryshev@gmail.com.

Information about the authors

Pukhir H., senior lecturer, department of information protection, Educational Institution "Belarusian State University of Informatics and Radioelectronics", puhir@bsuir.by.

Sheryshev R., student of group 561401, faculty of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", romasheryshev@gmail.com.

УДК 004.021+ 004.056.55+621.382.2:[621.315.592.3+620.192.63]

ИССЛЕДОВАНИЕ ТЕРМОКОМПЕНСАЦИИ ШУМОВЫХ ДИОДОВ ДЛЯ ИСПОЛЬЗОВАНИЯ В УСТРОЙСТВАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Д.О. Петров¹, В.В. Буслюк^{1,2}, О.О. Латий^{1,2}, В.А. Емельянов³

¹ Учреждение образования «Брестский государственный технический университет», г. Брест, Республика Беларусь

²ОАО «Цветотрон», г. Брест, Республика Беларусь

³ОАО «ИНТЕГРАЛ» - управляющая компания холдинга «ИНТЕГРАЛ», г. Минск, Республика Беларусь

Аннотация. Проведено исследование температурной стабилизации шумовых диодов для применения в устройствах промышленного интернета вещей (IIoT). Объектами исследования служили кремниевые планарные шумовые диоды производства ОАО «Цветотрон». Предложен метод термокомпенсации на основе последовательного встречного включения двух диодов. Экспериментально подтверждено, что использование данного метода позволяет стабилизировать шумовые параметры (спектральную плотность напряжения шума, граничную частоту) в расширенном диапазоне температур до +125 °С. Полученные результаты обеспечивают возможность применения шумовых диодов в качестве физических источников энтропии для криптографических систем IIoT.

Ключевые слова: термокомпенсация; шумовой диод; промышленный интернет вещей; интернет вещей; IIoT; IIoT; криптография; защита данных; физический источник энтропии; генератор случайных чисел.

INVESTIGATION OF THERMAL COMPENSATION OF NOISE DIODES FOR USE IN INDUSTRIAL INTERNET OF THINGS DEVICES

D.O. Petrov¹, V.V. Buslyuk^{1,2}, O.O. Latii^{1,2}, V.A. Emelyanov³

¹ Educational Institution "Brest State Technical University",
Brest, Republic of Belarus,

²Tsvetotron JSC, Brest, Republic of Belarus,

³INTEGRAL JSC – managing company of the INTEGRAL holding, Minsk,
Republic of Belarus

Abstract. This study investigates the temperature stabilization of noise diodes for use in Industrial Internet of Things (IIoT) devices. Silicon planar noise diodes were tested in the temperature range up to +125°C. A thermal compensation method using back-to-back series connection of two diodes was proposed and evaluated. The results demonstrate that this approach stabilizes noise parameters, including noise voltage spectral density and cutoff frequency, within acceptable limits at elevated temperatures. The proposed method expands the operating temperature range of noise diodes, enabling their use as physical entropy sources in random number generators for IIoT security applications.

Keywords: thermal compensation; noise diode; industrial internet of things; internet of things; IoT; IIoT; cryptography; data protection; physical entropy source; random number generator.

Введение

Интернет вещей (IoT, Internet of Things) представляет собой систему объединенных компьютерных сетей и подключенных электронных устройств со встроенными датчиками и программным обеспечением (ПО) для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека [1]. В свою очередь под промышленным интернетом вещей (Industrial Internet of Things, IIoT) следует понимать систему объединенных компьютерных сетей и подключенных промышленных электронных устройств со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека [2]. К электронным устройствам, составляющим промышленный интернет вещей, предъявляются повышенные требования в области кибербезопасности и отказоустойчивости [3, 4]. Одним из способов повышения безопасности процесса обмена данными между устройствами, входящими в состав IIoT, является криптографическая защита передаваемой информации современными симметричными и асимметричными методами шифрования, криптостойкость которых может быть повышена использованием физических источников энтропии для истинно случайной генерации ключей шифрования [7]. В качестве физических источников энтропии в системах защиты информации достаточно распространено использование шумовых полупроводниковых диодов (ШД), работающих в режиме лавинного пробоя [7]. В условиях воздействия на промышленные электронные устройства изменяющейся в широких пределах температуры особенно важно решение задачи стабилизация вольтамперных (ВАХ) и динамических характеристик полупроводниковых приборов и интегральных микросхем. Тем более, что большинство выпускаемых ШД предназначены для работы при температурах не более +70°C. Установление зависимости параметров шумовых диодов, таких, как напряжение пробоя, спектральная плотность напряжения шума, граничная

частота от температуры, а также разработка метода снижения температурного коэффициента спектральной плотности напряжения шума ШД является актуальной задачей отечественного производства.

Экспериментальная установка и методы измерений

В качестве объектов исследования использованы кремниевые планарные шумовые диоды производства ОАО «Цветотрон» (Республика Беларусь). Эти диоды успешно используются для формирования случайных числовых последовательностей, в метрологических целях для оценки каналов беспроводной связи, а также для маскирования побочных электромагнитных излучений [6,7]. Для обеспечения термостабилизации ШД использовался вариант последовательного включения двух шумовых диодов, включенных навстречу друг другу.

Исследования ШД проводились с применением компьютеризированной лабораторной установки В-300-БрГТУ (УП «Унитехпром БГУ», Республика Беларусь), предназначенной для экспериментального исследования физических процессов в электронных приборах и усилительных устройствах.

Установка имеет в своем составе встроенные электронные цифровые измерительные модули: двухканальный осциллограф, генератор и измеритель напряжений/токов, позволяющие наблюдать формы и измерять параметры электрических сигналов исследуемых электронных схем и компонентов во временном и частотном (спектральном) представлении, а также содержит в своем составе выносной термостатированный модуль для обеспечения нагрева исследуемых электронных приборов.

Методика измерения и расчета шумовых параметров соответствовала техническим условиям (ТУ) на шумовые диоды ТУ ВУ 200007171.038-2008.

Структурная схема регистрации и измерения переменного шумового сигнала ШД представлена на рисунке.

В качестве объектов исследования использованы кремниевые планарные шумовые диоды производства ОАО «Цветотрон» (Республика Беларусь). Эти диоды успешно используются для формирования случайных числовых последовательностей, в метрологических целях для оценки каналов беспроводной связи, а также для маскирования побочных электромагнитных излучений [6,7]. Для обеспечения термостабилизации ШД использовался вариант последовательного включения двух шумовых диодов, включенных навстречу друг другу.

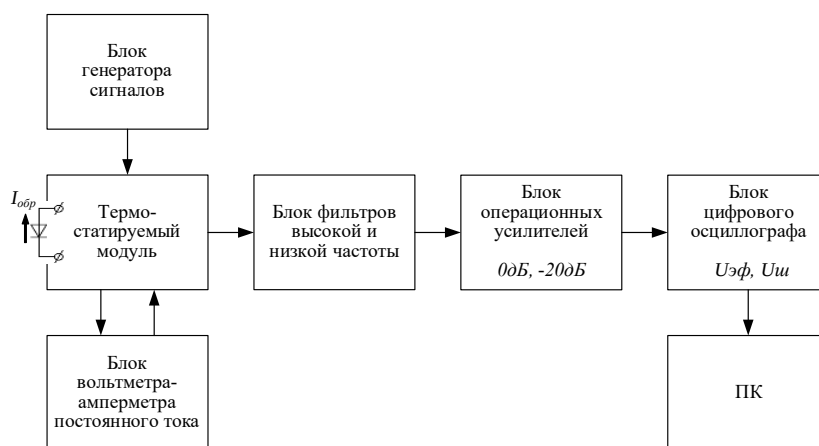
Исследования ШД проводились с применением компьютеризированной лабораторной установки В-300-БрГТУ (УП «Унитехпром БГУ», Республика Беларусь), предназначенной для

экспериментального исследования физических процессов в электронных приборах и усилительных устройствах.

Установка имеет в своем составе встроенные электронные цифровые измерительные модули: двухканальный осциллограф, генератор и измеритель напряжений/токов, позволяющие наблюдать формы и измерять параметры электрических сигналов исследуемых электронных схем и компонентов во временном и частотном (спектральном) представлении, а также содержит в своем составе выносной термостатированный модуль для обеспечения нагрева исследуемых электронных приборов.

Методика измерения и расчета шумовых параметров соответствовала техническим условиям (ТУ) на шумовые диоды ТУ ВУ 200007171.038-2008.

Структурная схема измерения переменного шумового сигнала ШД представлена на рисунке.



Структурная схема измерения переменного шумового сигнала диода
Block diagram of the diode AC noise signal measurement

Результаты измерения и их обсуждение

Ранее, в работе [8] исследованы ВАХ шумовых диодов ND102L, ND103L и ND104L в интервале температур от минус 25°C до + 35°C. Представленные в работе зависимости напряжения пробоя от температуры исследованных шумовых диодов носят линейный характер.

В связи с тем, что верхним пределом эксплуатации большинства кремниевых полупроводниковых приборов является температура +125°C, была произведена оценка смещения прямой и обратной ветвей ВАХ ШД ND103L при температурах +25°C, +70°C и +125°C

Проведены исследования партии из 20 шумовых диодов, работающих в условиях повышенных температур и не содержащих

в конструкции специальных термостабилизирующих элементов. Затем изучены 10 последовательно-парных сборок, сформированных из этих же шумовых диодов, при этом один диод в паре включался в прямом, а другой – в обратном направлении.

В таблице представлены средние значения шумовых параметров последовательной симметричной сборки ШД из этих же приборов при температурах 25°C, 70°C, 125°C. Как следует из таблицы, спектральная плотность напряжения шума, при норме ТУ не менее 30 мкВ / Гц $1/2$, а также граничная частота, при норме не менее 1МГц, не выходит за пределы установленных граничных значений.

Значения шумовых параметров последовательной симметричной сборки ШД ND103
при температуре 25°C, 70°C, 125°C
Noise parameter values of the series symmetric assembly of ND103 noise diodes at
temperatures of 25°C, 70°C, and 125°C

	Наименование и обозначение параметра											
	спектральная плотность напряже- ния шума (СПНШ)			нелинейность СПНШ			граничная частота шумового сигнала			эффективное напряжение шума		
	S_U , мкВ / Гц $^{1/2}$			δS_U , дБ			$f_{гр}$, МГц			$U_{эф}$, мВ		
	25°C	70°C	125°C	25°C	70°C	125°C	25°C	70°C	125°C	25°C	70°C	125°C
Сре днее знач ение	121,7	97,2	76,0	1,68	1,66	1,69	3,833	3,077	2,522	238,5	170,2	120,2

Заключение

Проведенные исследования показали, что повышение температуры приводит к изменению шумовых характеристик ШД. Несмотря на снижение эффективного напряжения шума, граничной частоты и спектральной плотности напряжения шума, температурная стабилизация напряжения пробоя прямосмещенным р-п-переходом ШД ND103L способствует стабилизации шумовых параметров в диапазоне температур до +125°C. Использование предложенного метода термокомпенсации позволит расширить температурный диапазон применения ШД для использования в физических генераторах случайных чисел устройств промышленного интернета вещей.

Список использованных источников

1. Довгаль В.А., Довгаль Д.В. (2018) Интернет Вещей: концепция, приложения и задачи. *Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки*. 1(212), 37–40.
2. Гринева Н.В., Абдикеев Н.М. (2025) Промышленный интернет вещей как основа интеллектуального производства. *Computational Nanotechnology*. 3(12), 96–104.

3. Alotaibi B. (2023) A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. *Sensors*. 23(17), 7470, 1–49.
4. Alabadi M., Habbal A., Wei X. (2022) Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions. *IEEE Access*. 10(1), 66374–66400.
5. Hameedi S.S., Bayat O. (2022) Improving IoT Data Security and Integrity Using Lightweight Blockchain Dynamic Table. *Appl. Sci*. 12, 9377, 1–18.
6. Буслюк В.В., Видрицкий А.Э., Голосов Д.А. и др. (2024) *Технологические аспекты производства изделий субмикронной электроники*. Минск, Бестпринт, Гл. 5, 162–200.
7. Петров Д.О., Буслюк В.В., Дереченник С.С., Емельянов В.А. (2023) Шумовые диоды как источник энтропии для аппаратных генераторов случайных чисел. *Безопасность информационных технологий*. 4, 137–149.
8. Zenevich A.O., Kochergina O.V., Buslyuk V.V., Fedosyuk D.N., Lushchy D.A. (2024) On the Temperature Characteristics of Noise Diodes. *Semiconductors*. 13, 1128–1131.

References

1. Dovgal V.A., Dovgal D.V. (2018) The Internet of Things: concept, applications, and challenges. *Bulletin of Adyge State University. Series 4: Natural-Mathematical and Technical Sciences*. 1(212), 37–40 (in Russian).
2. Grineva N.V., Abdikeev N.M. (2025) Industrial Internet of Things as a foundation for intelligent manufacturing. *Computational Nanotechnology*. 3(12), 96–104 (in Russian).
3. Alotaibi B. (2023) A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. *Sensors*. 23(17), 7470, 1–49.
4. Alabadi M., Habbal A., Wei X. (2022) Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions. *IEEE Access*. 10(1), 66374–66400.
5. Hameedi S.S., Bayat O. (2022) Improving IoT Data Security and Integrity Using Lightweight Blockchain Dynamic Table. *Appl. Sci*. 12, 9377, 1–18.
6. Buslyuk V.V., Vidritsky A.E., Golosov D.A. et al. (2024) *Technological aspects of manufacturing submicron electronics products*. Minsk, Bestprint, Ch. 5, 162–200 (in Russian).
7. Petrov D.O., Buslyuk V.V., Derechennik S.S., Emelyanov V.A. (2023) Noise diodes as a source of entropy for hardware random number generators. *Information Technology Security*. 4, 137–149 (in Russian).
8. Zenevich A.O., Kochergina O.V., Buslyuk V.V., Fedosyuk D.N., Lushchy D.A. (2024) On the Temperature Characteristics of Noise Diodes. *Semiconductors*. 13, 1128–1131.

Сведения об авторах

Петров Д.О., канд. техн. наук, доц., доцент кафедры ЭВМ и систем, Учреждение образования «Брестский государственный технический университет», polegdo@gmail.com.

Буслюк В.В., канд. техн. наук, доц., доцент кафедры ЭВМ и систем Брестского государственного технического университета, ведущий инженер-конструктор ОАО «Цветотрон», vbusliuk58@gmail.com.

Латий О.О., магистр техн. наук, главный конструктор ОАО «Цветотрон», nauka@tsvetotron.com.

Емельянов В.А., д-р техн. наук, проф., главный специалист по науке ОАО «Интеграл», emeljnov@bk.ru.

Information about the authors

Petrov D.O., Cand. Sci. (Techn.), Associate Professor, Associate Professor of the Department of Computer Engineering and Systems, Educational Institution "Brest State Technical University", Brest, Republic of Belarus, polegdo@gmail.com.

Buslyuk V.V., Cand. Sci. (Techn.), Associate Professor, Associate Professor of the Department of Computer Engineering and Systems, Brest State Technical University, Lead Design Engineer, Tsvetotron JSC, vbusliuk58@gmail.com.

Latii O.O., Master Sci. (Techn.), Chief Designer, Tsvetotron JSC, nauka@tsvetotron.com.

Emelyanov V.A., Dr. Sci. (Techn.), Professor, Chief Science Specialist, Integral JSC, emeljnov@bk.ru.

УДК 621.315.5/6

АНТИОТРАЖАЮЩИЕ ПОКРЫТИЯ НА ОСНОВЕ УГЛЕРОДНЫХ НАНОТРУБОК ДЛЯ ФОТОЧУВСТВИТЕЛЬНЫХ УСТРОЙСТВ

Н.Г. Ковальчук¹, Е.А. Дронина¹, Л.П. Томашевич¹, А.В. Петров², Н.А. Каланда², С.К. Лазарук¹

¹ Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

² НППЦ НАН Беларуси по материаловедению, г. Минск, Республика Беларусь

Аннотация. Разработан метод формирования антиотражающих покрытий на основе углеродных нанотрубок. Метод основан на химическом осаждении из газовой фазы, состоящей из аргона, паров этанола и раствора железосодержащего катализатора феррацена при температурах в реакторе до 200°C. Исследования спектров комбинационного рассеивания света и электронной микроскопии показали наличие одностенных углеродных нанотрубок в синтезированных пленках. Спектры зеркального отражения показали менее 1% от падающего светового сигнала.

Ключевые слова: антиотражающие покрытия; углеродные нанотрубки; спектры отражения; наноструктуры; осаждение из газовой фазы.

CARBON NANOTUBE-BASED ANTI-REFLECTIVE COATINGS FOR PHOTONSENSITIVE DEVICES

N.G. Kovalchuk¹, E.A. Dronina¹, L.P. Tomashevich¹, A.V. Petrov², N.A. Kalanda², S.K. Lazarouk¹

¹ Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

² Scientific-Practical Materials Research Centre of the NAS of Belarus, Minsk, Republic of Belarus

Abstract. A method for forming antireflective coatings based on carbon nanotubes has been developed. The method is based on chemical vapor deposition, consisting of argon, ethanol

vapor, and a solution of iron-containing ferracene catalyst at reactor temperatures of up to 200°C. Raman and electron microscopy studies revealed the presence of single-walled carbon nanotubes in the synthesized films. Specular reflectance spectra showed less than 1% of the incident light signal.

Keywords: anti-reflective coatings; carbon nanotubes; reflectance spectra; nanostructures; chemical vapor deposition.

Антиотражающие покрытия используются для управления световым сигналом в различных оптоэлектронных фоточувствительных устройствах [1-8]. Также поглощение оптического сигнала востребовано с целью маскирования объектов при их обнаружении за счет регистрации отраженного электромагнитного сигнала, что позволяет относить антиотражающие покрытия к техническим средствам защиты информации.

В данной работе проведено исследование антиотражающих свойств пленок на основе углеродных нанотрубок, сформированных химическим осаждением из газовой фазы на титановые подложки.

Химическое осаждение углеродных нанотрубок из газовой фазы проводилось в реакторе, включающем как горячую (1050 °C), так и холодную зоны (< 200 °C). Рабочий газ аргон вместе с парами этанола и раствора железосодержащего катализатора феррацена подавались в горячую зону реактора, после чего в холодной зоне на кремниевых подложках были сформированы пленки из одностенных углеродных нанотрубок (ОСУНТ). После охлаждения до комнатной температуры поверхность пленок из ОСУНТ обрабатывали этанолом для увеличения плотности массива нанотрубок в пленке и улучшения их адгезии к титановым подложкам. Структура сформированных пленок из ОСУНТ исследовались с помощью спектроскопии комбинационного рассеяния света и электронной микроскопии. Спектры отражения измерялись при помощи спектрометра Proscan MC 122.

Исследование спектров комбинационного рассеивания в исследуемых пленках показало наличие характерного G-пика, D-пика, 2D-пика и пиков RBM моды, что свидетельствует о присутствии одностенных углеродных трубок в синтезированных пленках. Углеродные нанотрубки имеют нитевидную структуру с диаметром нитей нанометрового диапазона. Спектры измеряли как в режиме зеркального отражения, так и в режиме диффузионного отражения с учетом диффузионного рассеяния. При зеркальном отражении регистрируется менее 1% от падающего светового сигнала, в то время как диффузное отражение регистрируется в диапазоне 4-5%, что свидетельствует о диффузном рассеивании падающего светового сигнала. Тем не менее, достигнутые уровни отражения свидетельствуют о высокой эффективности функционирования исследуемых пленок в качестве антиотражающих покрытий, что представляет интерес для их использования в различных электронных устройствах.

Таким образом, разработан метод формирования антиотражающих покрытий на основе углеродных нанотрубок для снижения отражения оптического сигнала, что может быть использовано для управления световыми потоками в устройствах интегральной оптики, а также при маскировании объектов в качестве технических средств защиты информации.

Работа выполнена при финансовой поддержке БРФФИ (проект № T25ИНДА-004).

Список использованных источников / References

1. Monica S. La, Maiello G., Ferrari A., Masini G., Lazarouk S., Jaguiro P., et al. (1997) Progress in the field of integrated optoelectronics based on porous silicon. *Thin Solid Films*. 297 (1-2), 265-267.
2. Lazarouk S.K., Leshok A.A., Kozlova T.A., Dolbik A.V., Vi L.D., Ilkov V.K., et al. (2019) 3D Silicon Photonic Structures Based on Avalanche LED with Interconnections Through Optical Interposer. *International Journal of Nanoscience*. 18 (3-4), 1940091.
3. Lazarouk S., Bondarenko V., Pershukevich P., Monica S. La, Maiello G. (1994) Visible Electroluminescence from Al-Porous Silicon Reverse Bias Diodes Formed on the Base of Degenerate n-Type Silicon. *MRS Online Proceedings Library Archive*. 358, 659-664.
4. Lazarouk S. K., Sasinovich D. A., Katsuba, P. S., Labunov V. A., Leshok A. A., Borisenko V. E. (2007) Electroluminescence from nanostructured silicon embedded in anodic alumina. *Semiconductors*. 41 (9), 1109-1112.
5. Bertolotti M., Carassiti F., Fazio E., Ferrari A., Monica S. La, Lazarouk S., et al. (1995) Porous silicon obtained by anodization in the transition regime. *Thin Solid Films*. 255 (1-2), 152-154.
6. Lazarouk S., Jaguiro P., Katsouba S., Monica S. La, Maiello G., Masini G., et al. (1996) Visible light from aluminum-porous silicon Schottky junctions. *Thin Solid Films*. 276 (1-2), 168-170.
7. Lazarouk S., Jaguiro P., Katsouba S., Masini G., Monica S. La, Maiello G., et al. (1996) Stable electroluminescence from reverse biased n-type porous silicon-aluminum Schottky junction device. *Applied Physics Letters* 68, 2108-2110.
8. Lazarouk S., Muravski A., Sasinovich D., Chigrinov V., Kwok H. S. (2007) Porous and pillar structures formed by anodization for vertical alignment of nematic liquid crystal. *Japanese Journal of Applied Physics*. 46 (10R), 6889.

Сведения об авторах

Ковальчук Н.Г., старший научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Дронина Е.А., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Томашевич Л.П., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Петров А.В., кандидат физико-математических наук, доцент, старший научный сотрудник, Научно-практический центр НАН Беларуси по материаловедению, petrov@physics.by.

Каданда Н.А., доктор физико-математических наук, доцент, ведущий научный сотрудник, Научно-практический центр НАН Беларуси по материаловедению, kalanda@physics.by.

Лазарук С.К., доктор физико-математических наук, профессор, заведующий НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», serg@nano.bsuir.edu.by.

Information about the authors

Kovalchuk N., Senior Researcher, Research Lab 4.6, Educational Institution "Belarusian State University of Informatics and Radioelectronics"

Dronina E., Researcher, Research Lab 4.6, Educational Institution "Belarusian State University of Informatics and Radioelectronics"

Tomashevich L., Researcher, Research Lab 4.6, Educational Institution "Belarusian State University of Informatics and Radioelectronics".

Petrov A., PhD (Physics and Mathematics), Associate Professor, Senior Researcher, Scientific and Practical Center for Materials Science, National Academy of Sciences of Belarus.

Kadanda N., DSc (Physics and Mathematics), Associate Professor, Leading Researcher, Scientific and Practical Center for Materials Science, National Academy of Sciences of Belarus, kalanda@physics.by.

Lazarouk S., DSc (Physics and Mathematics), Professor, Head of Research Lab 4.6, Educational Institution "Belarusian State University of Informatics and Radioelectronics", serg@nano.bsuir.edu.by.

УДК 614.841

ПРОТИВОДЫМНАЯ ЗАЩИТА МНОГОЭТАЖНЫХ ЗДАНИЙ

В.Е. Галузо, А.И. Пинаев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В многоэтажных зданиях для обеспечения незадымляемости путей эвакуации при пожаре, согласно нормативным документам, должна быть система противодымной защиты. В состав этой системы входит система компенсирующей подачи воздуха. Для обеспечения эффективности системы противодымной защиты предлагается осуществлять естественную компенсирующей подачи воздуха не по вертикальным вентиляционным шахтам, а по горизонтальным воздуховодам.

Ключевые слова: пожарная безопасность; противодымная защита; противодымная вентиляция; многоэтажные здания; эвакуация; дымоудаление; компенсирующая подача воздуха.

SMOKE PROTECTION OF MULTI-STORY BUILDINGS

V.E. Galuzo, A.I. Pinaev

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. In multi-story buildings, to ensure smoke-free escape routes during a fire, regulations require a smoke control system. This system includes a compensating air supply

system. To ensure the effectiveness of the smoke control system, it is proposed to provide the compensating air supply through horizontal ducts rather than vertical ventilation shafts.

Key words: fire safety; smoke protection; smoke ventilation; multi-story buildings; evacuation; smoke removal; compensating air supply.

Введение

Согласно [1] во всех многоэтажных зданиях любого функционального назначения должна быть вентиляционная система противодымной защиты (ПДЗ). Система ПДЗ должна обеспечить нераспространение дыма и незадымляемость путей эвакуации при пожаре, что в свою очередь должно способствовать беспрепятственной эвакуации из зданий в кратчайшие сроки. Основной составляющей системы ПДЗ многоэтажных зданий согласно [1] является система дымоудаления из коридора этажа пожара. Однако, как было отмечено в [2], при запуске системы ПДЗ дымоудаления из коридора не происходит до тех пор, пока не будут открыты двери из коридора на лестничную клетку. Открыть двери на лестничную клетку могут люди, эвакуирующиеся с этажа пожара, а это значит, что выходить из помещений, они будут в задымленный коридор, в котором согласно [1] температура дыма 300 °С. При этом не понятно, как свои функции оповещения о пожаре и управления эвакуацией будут исполнять технические средства, размещенные в коридоре, максимальная температура эксплуатации которых не превышает 55 °С [3].

Основная часть

Если, рассчитать параметры вентиляционной системы дымоудаления из коридора в соответствии с примерами, приведенными в [1,4], то перепады давления на закрытых дверях путей эвакуации, нормируемые [5], будут очень большими, что будет препятствовать эвакуации.

Поэтому в [2] впервые была предложена, а затем в [1,4] прописана необходимость использования компенсирующей подачи воздуха в коридор при пожаре.

В соответствии с [1, 4] способы подачи воздуха могут быть различными, но в основном подразделяются на использование принудительной и естественной вентиляции. При этом анализ проектных решений показывает, что на практике оба варианта используются одинаково часто. Компенсирующая подача воздуха осуществляется по вертикальным вентиляционным шахтам с использованием вентилятора или без него.

В ходе аэродинамических испытаний вентиляционных систем ПДЗ обнаруживается, что естественная компенсирующая подача не выполняет свои функции. В частности, в зимний отапливаемый период года в шахтах

естественной компенсирующей подачи воздуха имеет место сильная прямая тяга из-за чего на первых этажах зданий имеет место большой перепад давления на закрытых дверях путей эвакуации. Эта тяга в 25-ти этажных зданиях высотой 75 м при температуре воздуха в коридоре здания 20°C (удельном весе 12 н/м^3) и наружного воздуха – 20°C (удельном весе 10 н/м^3) составляет около 150 Па. А это означает, что для того чтобы воздух пошел снаружи в коридор надо опрокинуть тягу создав в коридоре разряжение равное 150 Па. А это значение разряжения воздуха в коридоре является критическим так как перепад давления на закрытых дверях путей эвакуации не должно быть более 150 Па. То есть эта компенсация не эффективна и более того усугубляет ситуацию.

Кроме того, следует добавить и то обстоятельство, что согласно [1, 4] в коридоре, как отмечалось выше, при пожаре температура 300°C (удельный вес 6 н/м^3), а это означает что разряжение в коридоре за счет естественной компенсации в этом случае будет еще больше и составит около 450 Па.

Заключение

Рекомендуется не использовать при проектировании вентиляционных систем ПДЗ естественной компенсирующей подачи воздуха по вертикальным шахтам. Проектировать естественную компенсацию только по горизонтальным воздуховодам, в которых отсутствует прямая тяга, как это было рекомендовано в [2] и уже реализовано в проектных решениях, которые нашли подтверждение их правильности в ходе аэродинамических испытаний. Горизонтальные воздуховоды следует размещать непосредственно над дверями эвакуационных выходов на лестничные клетки. Тем самым обеспечивается пониженная температура воздуха над дверями, равная наружной температуре воздуха. А это значит, что температура воздуха над дверью, где размещаются свето-речевые оповещатели, не будет превышать их максимальную температуру эксплуатации.

Список использованных источников

1. СН 2.02.07-2020. Противодымная защита зданий и сооружений при пожаре. Системы вентиляции.
2. Галузо В.Е., Литвинова О.Е. Дымоудаление: задачи и их решение. Производственно-практический журнал «Служба спасения 01-2011», №9, 2011, с.42-43.
3. ООО «Авангардспецмонтажплюс». Оповещатели пожарные серии «АСТО». Руководство по эксплуатации.
4. ТКП 45-4.02-273-2012. Противодымная защита зданий и сооружений при пожаре. Системы вентиляции.
5. НПБ 23-2010*. Противодымная защита зданий и сооружений. Методы приемосдаточных и периодических испытаний.

References

1. SN 2.02.07-2020. Smoke protection of buildings and structures in case of fire. Ventilation systems.
2. Galuzo V.E., Litvinova O.E. Smoke extraction: tasks and their solution. Industrial and practical magazine "Rescue Service 01-2011", No. 9, 2011, pp.42-43.
3. Avangardspetsmontazhplus LLC. Fire alarm systems of the "ASTO" series. User manual.
4. ТКР 45-4.02-273-2012. Smoke protection of buildings and structures in case of fire. Ventilation systems.
5. NPB 23-2010*. Smoke protection of buildings and structures. Methods of acceptance and periodic tests.

Сведения об авторах

Галузо В.Е., канд. техн. наук, доц., доцент, Белорусский государственный университет информатики и радиоэлектроники, valga51@yandex.ru.

Пинаев А.И., канд. техн. наук, доц., доцент, Белорусский государственный университет информатики и радиоэлектроники, info@avsm.by.

Information about the authors

Galuzo V.E., Ph.D. (Eng.), Assoc. Prof., Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", valga51@yandex.ru.

Pinaev A.I., Ph.D. (Eng.), Assoc. Prof., Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", info@avsm.by.

УДК 614.841

ПРОТИВОДЫМНАЯ ЗАЩИТА ПАРКИНГА

В.Е. Галузо, А.И. Пинаев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В паркингах согласно нормативным документам должна быть системами оповещения людей о пожаре и управления эвакуацией. Для обеспечения эвакуации в кратчайшие сроки в паркингах должна быть противодымная защита (ПДЗ). Приводится обоснование того, что в случае эвакуации из паркинга за время, не превышающее времени заполнения резервуара дыма, система ПДЗ не нужна. Предлагаемое техническое решение позволит существенно снизить затраты на строительство паркингов.

Ключевые слова: пожарная безопасность; паркинг; эвакуация; противодымная защита; дымоудаление; подпор воздуха; тамбур-шлюз.

SMOKE PROTECTION FOR PARKING

V.E. Galuzo, A.I. Pinaev

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. According to regulations, parking lots must be equipped with fire warning and evacuation management systems. To ensure prompt evacuation, parking lots must be equipped with smoke protection systems (SPS). It is argued that if the parking lot is evacuated within a timeframe not exceeding the time it takes for the smoke reservoir to fill, a SPS system is not necessary. The proposed technical solution will significantly reduce parking lot construction costs.

Key words: fire safety; parking; evacuation; smoke protection; smoke removal; air pressurization; vestibule-airlock.

Введение

В соответствии с [1] паркинги следует оборудовать системами оповещения людей о пожаре и управления эвакуацией (СОПиУЭ), которая запускается от сработки дымовых извещателей пожарных (ДИП) системы пожарной сигнализации. Согласно [1,2] для обеспечения нормальных условий эвакуации в кратчайшие сроки в паркингах закрытого типа должно осуществляться удаление продуктов горения (ДУ) при пожаре с использованием вентиляционных систем противодымной защиты (ПДЗ) с механическим побуждением. Кроме ДУ из паркинга, согласно [1], в лестничных клетках и шахтах лифтов следует предусматривать подпор воздуха при пожаре или устройство на всех этажах тамбуров-шлюзов 1 типа с подпором воздуха.

Основная часть

В [3] было отмечено, что в соответствии с [2] помещение паркинга, подлежащее оборудованию ПДЗ, должно быть разделено на дымовые зоны (резервуары дыма) с учетом возможности возникновения пожара в одной из них. Каждая дымовая зона (ДЗ) должна быть ограждена строительными конструкциями, выступающими от перекрытия к полу, не ниже чем 2 м от пола и образующими под перекрытием резервуары дыма. Минимальную глубину дымовой зоны (резервуара дыма) следует принимать 0,5 м. Согласно [3] время заполнения такого резервуара дыма от появления возгорания составляет около 260 с.

Время сработки ДИП на практике не более 80 с [4]. А это значит, что от сработки ДИП и запуска СОПиУЭ до заполнения резервуара дыма пройдет около 180 с. Расстояние от наиболее удаленной точки ДЗ (площадь ДЗ согласно [2] 3000 м²) до ее края не превышает 30 м. При скорости эвакуации в горизонтальной плоскости паркинга равной 60 м/мин это расстояние может быть преодолено за 30 с. То есть эвакуация из ДЗ произойдет до заполнения резервуара дыма, а значит ДУ для обеспечения эвакуации не нужна. Это положение нашло свою реализацию в проекте системы ПДЗ паркинга, сданного в эксплуатацию в конце 2025 г.

Однако, на этом объекте, при исключении системы ДУ, тем не менее были реализованы две системы подпора воздуха в тамбур-шлюзы 1 типа перед входами из паркинга в лестничную клетку и лифты.

Эвакуационная лестничная клетка связывает паркинг и наружное пространство. Протяженность этой лестницы, не связанной с пространством паркинга, эквивалентна двум этажам паркинга и составляет величину около 15 м. То есть длина этой лестницы никак не подпадает под требование обеспечения ее незадымления. Скорость воздуха в дверном проеме тамбур-шлюза согласно [2] при совместном действии ДУ из паркинга и подпора воздуха в тамбур-шлюз не менее 1,3 м/с. Но это невозможно так как нет ДУ. Более того дым опустится до верхней отметки дверного проема до того, как из паркинга эвакуируются люди и в лестницу никто не будет входить.

Если здание, расположенное над паркингом высотой более 30 м, то в соответствии с [2] в нем будет ПДЗ и соответственно подпор воздуха в шахты лифтов. При программировании систем пожарной автоматики здания и паркинга будет прописано включение подпора воздуха в шахты лифтов здания и дым из паркинга не пойдет по шахте лифтов.

Заключение

Таким образом, при проектировании системы противопожарной защиты паркинга и расположенного над ним многоэтажного здания нет необходимости в оборудовании паркинга системой дымоудаления и подпора воздуха в тамбур-шлюз перед эвакуационной лестнице выхода из паркинга наружу поскольку время заполнения резервуара дыма при пожаре в паркинге больше времени эвакуации из паркинга. Кроме того, нет необходимости в подпоре воздуха в тамбур-шлюз перед лифтами в паркинге, если над паркингом расположено многоэтажное здание, поскольку в этом здании будет подпор воздуха в лифтовые шахты, который не пустит в него дым из паркинга. Это техническое решение позволит снизить стоимость строительства многоэтажных зданий с встроенными паркингами.

Список использованных источников

1. СН 3.02.03-2019 Станции технического обслуживания транспортных средств. Гаражи-стоянки автомобилей.
2. СН 2.02.07-2020 Противодымная защита зданий и сооружений при пожаре. Системы вентиляции.
3. Галузо В.Е., Калита О.В., Пинаев А.И. Тактика противопожарной защиты многоэтажных гаражей-стоянок // Технические средства защиты информации: тезисы докладов XX Белорусско-российской научно-технической конференции., / БГУИР. – Минск, 2022

4. Хорошко В.В. Эффективность электронных систем пожарной безопасности в зоне горения автомобилей для подземных гаражей – стоянок жилых зданий. Доклады БГУИР. 2020; 18(7): 63-70.

References

1. SN 3.02.03-2019 Vehicle service stations. Parking garages
2. SN 2.02.07-2020 Smoke Protection of Buildings and Structures in Case of Fire. Ventilation Systems.
3. Galuzo V.E., Kalita O.V., Pinaev A.I. Fire Protection Tactics for Multi-Story Parking Garages // Technical Means of Information Protection: Abstracts of the XX Belarusian-Russian Scientific and Technical Conference. / BSUIR. – Minsk, 2022
4. Khoroshko V.V. Efficiency of Electronic Fire Safety Systems in the Car Combustion Zone for Underground Parking Garages of Residential Buildings. BSUIR Reports. 2020; 18(7): 63-70.

Сведения об авторах

Галузо В.Е., канд. техн. наук, доц., доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», valga51@yandex.ru.

Пинаев А.И., канд. техн. наук, доц., доцент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» info@avsm.by.

Information about the authors

Galuzo V.E., Ph.D. (Eng.), Assoc. Prof., Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", valga51@yandex.ru.

Pinaev A.I., Ph.D. (Eng.), Assoc. Prof., Associate Professor, Educational Institution "Belarusian State University of Informatics and Radioelectronics", info@avsm.by.

УДК 621.3.049.77:535.8

РАЗРАБОТКА КОНФИГУРАЦИИ СИСТЕМЫ ОСВЕЩЕНИЯ АВТОМАТИЧЕСКИХ ЗОНДОВЫХ УСТАНОВОК

Г.И. Грицкевич, В.Э. Пашкевич, Ю.А. Смолкин, Р.С. Жук,
А.С. Лешко, И.Ю. Ловшенко

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрена проблема конструктивных решений систем освещения автоматических зондовых установок для контроля полупроводниковых пластин. Проведен сравнительный анализ методов освещения. Обоснована комбинированная светодиодная конфигурация с кольцевой и боковой подсветкой, обеспечивающая точность и исключение термодеструкции.

Ключевые слова: зондовая установка, освещение, микроскопия, кольцевая подсветка, тестирование микросхем, светодиоды, поляризация, борьба с бликами, автоматизация.

DEVELOPMENT OF A LIGHTING SYSTEM CONFIGURATION FOR AUTOMATIC PROBE STATIONS

G. Gritskevich, V. Pashkevich, Y. Smolkin, R. Zhuk,
A. Leshko, I. Lovshenko

*Educational Institution "Belarusian State University of Informatics
and Radioelectronics", Minsk, Republic of Belarus*

Abstract. The problem of design solutions for lighting systems of automatic probe stations for semiconductor wafer inspection is considered. A comparative analysis of lighting methods is carried out. A combined LED configuration with ring and side illumination is substantiated, ensuring accuracy and thermal stability.

Keywords: probe station, illumination, microscopy, ring light, integrated circuit testing, light-emitting diodes (LED), polarization, glare control, automation.

Введение

Зондовые установки, обеспечивающие электрический контакт с тестовыми структурами и функционирующие в автоматическом режиме, исключают непосредственное визуальное участие оператора. В данных условиях система освещения перестает быть вспомогательным элементом и приобретает статус ключевого звена, определяющего точность работы применяемых алгоритмов компьютерного зрения. Масштаб контролируемых элементов (десятки микрометров) и зеркальная природа контактных площадок формируют сложную оптическую задачу [1]. Таким образом, целью работы является анализ существующих методов освещения и обоснование выбора оптимальной конфигурации для автоматизированного комплекса.

Основная часть

В микроскопии непрозрачных объектов применяются различные схемы освещения, каждая из которых имеет свои оптические особенности и области применения. Кольцевая подсветка представляет собой кольцо со светодиодами, которое крепится на объектив, обеспечивая коаксиальное бестеневое освещение. Сегментированные модели позволяют программно включать отдельные сектора для создания направленного света [2]. Метод освещения темного пола использует источники, расположенные сбоку под острым углом и позволяет выявлять мельчайшие неровности рельефа благодаря образованию теней, делая дефекты отчетливо видимыми. Вертикальный осветитель вводит свет через полупрозрачное зеркало в оптический тракт микроскопа, обеспечивая освещение строго перпендикулярно поверхности, что идеально для ровных зеркальных

объектов, но требует сложной реализации. Купольное освещение с полусферическим рассеивателем создает максимально равномерный свет для объектов сложной формы.

Способы крепления должны обеспечивать стабильность и юстировку. Кольцевые подсветки крепятся непосредственно к объективу. Для бокового освещения оптимальны гибкие держатели, позволяющие менять положение источника.

Критическая проблема – блики от металлизированных поверхностей. Для борьбы с ними эффективен поляризационный метод, который заключается в установке фильтра на источник и анализатора перед объективом с перпендикулярными осями. Диффузоры превращают точечный источник в протяженный, снижая зеркальную составляющую. Профессиональные решения включают микролинзовые рассеиватели и специальные сорта акрила, например, опаловый.

Заключение

На основе анализа для автоматической установки предлагается комбинированная система. Базовым решением выбрана сегментированная кольцевая светодиодная подсветка с программным управлением. Она обеспечивает равномерное бестеневое освещение, необходимое для надежной работы алгоритмов компьютерного зрения при автоматическом наведении зондов на контактные площадки. Дополнительно применяются боковые светильники на гибких держателях с фокусирующими линзами. Они служат для специальных задач: нахождение дефектов, выявление рельефа методом косого освещения и работа с глубокими полостями. Выбор светодиодной технологии обусловлен ее преимуществами: отсутствие термодформаций, компактность, энергоэффективность, долговременная стабильность параметров и широкий диапазон регулировки яркости без изменения спектра [3]. Технические параметры должны обеспечивать освещенность не менее 24000 люкс, цветовую температуру 5600-6500 К, независимое управление каналами и наличие поляризационных фильтров. Предложенное решение обладает необходимой программной управляемостью и масштабируемостью для интеграции в существующие автоматизированные комплексы тестирования полупроводниковых пластин.

Список использованных источников

1. Dahoo P. R., Pougnet P., El Hami A. *Nanometer-scale Defect Detection Using Polarized Light*. – Hoboken: Wiley, 2016. – 336 p. – (Wiley Semiconductors Series).
2. Белашенков Н. Р., Лопатин А. И., Никифоров В. О., Нисенбаум И. А., Пряничников В. С. Осветительная система для микроскопа с регулируемой цветовой

температурой излучения // *Известия высших учебных заведений. Приборостроение*. – 2006. – Т. 49, № 10. – С. 67–70.

3. Martin G., Agostini H. T., Hansen L. L. Light emitting diode microscope illumination for green fluorescent protein or fluorescein isothiocyanate epifluorescence // *BioTechniques*. – 2005. – Vol. 38, No. 2. – P. 204–206.

References

1. Dahoo P. R., Pougnet P., El Hami A. *Nanometer-scale Defect Detection Using Polarized Light*. – Hoboken: Wiley, 2016. – 336 p. – (Wiley Semiconductors Series).

2. Belashenkov N. R., Lopatin A. I., Nikiforov V. O., Nisenbaum I. A., Pryannichnikov V. S. Illumination System for a Microscope with Adjustable Color Temperature of Radiation // *Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie*. – 2006. – Vol. 49, No. 10. – Pp. 67–70. (in Russian)

3. Martin G., Agostini H. T., Hansen L. L. *Light emitting diode microscope illumination for green fluorescent protein or fluorescein isothiocyanate epifluorescence* // *BioTechniques*. – 2005. – Vol. 38, No. 2. – P. 204–206.

Сведения об авторах

Грицкевич Г.И., студент 3-го курса учреждения образования «Белорусский университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, gritskevich.grigoriy@gmail.com.

Пашкевич Валерия Эдуардовна, студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pashkevitch.lera@gmail.com.

Смолкин Юрий Александрович, студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» alikkoval375@gmail.com.

Жук Роман Сергеевич, студент учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» dyzeex64b@gmail.com.

Лешко Александр Сергеевич, студент учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», leshhko05@gmail.com.

Ловшенко Иван Юрьевич, без степени, без звания, старший преподаватель кафедры микро- и наноэлектроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lovshenko@bsuir.by

Information about the authors

Gritskevich G, student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, gritskevich.grigoriy@gmail.com.

Pashkevich V, student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, pashkevitch.lera@gmail.com.

Smolkin Y, student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, alikkoval375@gmail.com.

Zhuk R, student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, dyzeex64b@gmail.com.

Leshko A, student, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, leshhko05@gmail.com.

Lovshenko I, Senior Lecturer, Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, lovshenko@bsuir.by.

УДК 004.056+003.26

АДАПТАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА, ОСНОВАННОГО НА ИЗМЕНЕНИИ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ, ДЛЯ ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ ФОРМАТА SVG

Н. И. Уласевич, М. Г. Савельева

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассмотрены два стеганографических подхода: модификация цветowych каналов пикселей растрованного документа и внедрение дополнительных элементов в векторные изображения SVG. Предложена адаптация метода, использующего полутоновые значения текстовых символов для выбора контейнерных элементов, к векторной графике. В качестве модифицируемых атрибутов выступают координаты центров эллипсов, скрытых под закрашенными областями. Встраивание битов сообщения осуществляется по правилу четности координат. Разработанные алгоритмы имеют линейную сложность и сохраняют визуальную целостность изображения.

Ключевые слова: стеганография; растровая графика; векторная графика; SVG; полутоновые значения; эллипс; адаптация алгоритма.

ADAPTATION OF A STEGANOGRAPHIC METHOD BASED ON SPATIAL DOMAIN MODIFICATION FOR SVG VECTOR IMAGES

N. I. Ulasevich, M. G. Savelieva

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. Two steganographic approaches are considered: modification of pixel color channels in a rasterized document and embedding additional elements into SVG vector images. An adaptation of the method that uses halftone values of text symbols to select container elements is proposed for vector graphics. The coordinates of ellipse centers hidden under filled areas serve as modifiable attributes. Message bits are embedded according to the parity rule of the coordinates. The developed algorithms have linear complexity and preserve the visual integrity of the image.

Keywords: steganography; raster graphics; vector graphics; SVG; halftone values; ellipse; algorithm adaptation.

Введение

Защита авторских прав и скрытая передача данных являются важными задачами в области информационной безопасности [1]. Стеганографические методы позволяют внедрять тайные сообщения

в объекты-контейнеры без заметного искажения их свойств. Перспективными контейнерами выступают как растровые, так и векторные изображения.

В работе [2] предложен метод скрытия информации в растровых изображениях, полученных после растривания векторных текстовых символов. Выбор пикселей для встраивания определяется сопоставлением их цветовых характеристик с ключевыми значениями. В методе [3] для векторных изображений SVG используется правило визуального ранжирования: дополнительные эллипсы, помещенные в начало документа, перекрываются закрашенными фигурами и становятся невидимыми, а информация кодируется в дробных частях угла и расстояния от ключевой точки.

Цель работы – адаптировать метод [2], основанный на полутоновых значениях текстовых символов и модификации по четности, для использования в векторных файлах SVG, что позволит объединить преимущества методов.

Основная часть

В работе [2] контейнером служит растровое изображение, полученное после растривания векторных текстовых символов с заданным разрешением. При растривании возникают полутоновые пиксели, контур буквы «расплывается», и общее количество пикселей увеличивается. Именно в эти новые пиксели предлагается встраивать информацию. Формируется массив пикселей, для которых значение выбранного цветового канала равно заданному эталону. Встраивание бита сообщения в другой цветовой канал осуществляется изменением четности значения: если бит не соответствует текущей четности, к значению прибавляется нечетное число (шаг изменения). Извлечение производится путем анализа четности значений того же цветового канала у тех же пикселей.

В работе [3] используется векторный формат SVG, основанный на XML и позволяющий описывать графические объекты с помощью математических координат. В документ добавляются эллипсы с малым радиусом, которые располагаются в коде до закрашенных фигур. Благодаря правилу визуального ранжирования такие эллипсы перекрываются вышележащими фигурами и не отображаются на экране. Центры эллипсов выбираются внутри многоугольников, полученных из исходных примитивов. Информация кодируется путем выбора позиций в дробных частях угла наклона прямой, соединяющей центр эллипса с ключевой точкой, и расстояния до нее.

Предлагается перенести ключевые принципы работы [2] – выбор элементов на основе полутоновых значений текстовых символов и встраивание битов по правилу четности – в векторную среду. В качестве

контейнера рассматривается SVG-документ, содержащий текстовые элементы и закрашенные векторные фигуры (прямоугольники, многоугольники и т.п.).

Для каждого текстового элемента (символа или его части) вычисляется числовое значение, которое является аналогом полутонового оттенка из растрового метода. В простейшем случае это может быть хеш-код от строки символа или значение яркости при виртуальном растривании с фиксированным разрешением. Задается эталонное значение. Если вычисленное значение совпадает с эталоном, то данный текстовый элемент выбирается для формирования точки-кандидата. В качестве такой точки используется, например, центр ограничивающего прямоугольника текстового элемента или точка, смещенная от него по диагонали (по аналогии с исходным методом, где брался пиксель, расположенный по диагонали от проверяемого).

В найденной точке создается эллипс с малым радиусом (например, 0,1 условных единиц). Этот эллипс добавляется в начало SVG-документа (чтобы оказаться под всеми закрашенными фигурами) и включается в массив эллипсов, предназначенных для встраивания. Таким образом, массив формируется на основе текстовых элементов, удовлетворяющих ключевому условию.

Скрываемое сообщение преобразуется в двоичную последовательность. Для каждого бита последовательно используется эллипс из сформированного массива. Выбор модифицируемого атрибута задается ключом. Правило встраивания: если бит сообщения равен единице, целая часть выбранной координаты должна быть нечетной; если бит равен нулю – четной. Если текущее значение уже удовлетворяет требуемой четности, изменение не производится. В противном случае к значению прибавляется нечетное число. Поскольку прибавляемое число нечетное, четность меняется на противоположную. Величина шага выбирается минимальной, чтобы изменение координаты было незаметным. Так как радиус эллипса крайне мал, а сам эллипс скрыт под закрашенной фигурой, даже заметное смещение его центра не будет обнаружено визуально.

Извлечение производится в обратном порядке. Из SVG-документа выбираются все эллипсы с радиусом, не превышающим заданный порог. Для каждого такого эллипса определяется значение выбранной. Четность целой части определяет бит сообщения: четное – ноль, нечетное – единица. Последовательность битов преобразуется в исходное сообщение. Если при встраивании использовалась служебная информация, например, длина сообщения, она извлекается аналогичным образом.

Заключение

Предложена адаптация стеганографического метода, первоначально разработанного для растровых изображений, к векторному формату SVG. В отличие от исходного подхода, где контейнером выступают пиксели, модификация переносится на координаты эллипсов, скрытых под закрашенными фигурами. Выбор эллипсов осуществляется на основе числовых характеристик текстовых элементов, что сохраняет принцип избирательности, свойственный исходному методу. Дальнейшие исследования могут быть направлены на оценку пропускной способности, устойчивости метода к атакам, а также на использование других векторных примитивов и атрибутов для увеличения емкости.

Список использованных источников

1. Урбанович П. П. (2016) *Защита информации методами криптографии, стеганографии и обфускации*. Минск, БГТУ.
2. Савельева М. Г. (2024) Метод стеганографического преобразования на основе изменения пространственной области растрованного документа-контейнера. *Веб-программирование и интернет-технологии (WebConf2024): материалы 6-й Междунар. науч.-практ. конф.*, 337–340.
3. Уласевич Н. И., Жилияк Н. А. (2025) Стеганографический метод на основе встраивания дополнительных элементов под закрашенные участки в изображениях в формате SVG. *Труды БГТУ. Сер. 3, Физико-математические науки и информатика*, (2), 76–82.

References

1. Urbanovich P. P. Information protection by cryptography, steganography and obfuscation methods. Minsk, BGTU Publ., 2016. 220 p. (In Russian).
2. Savelyeva M. G. Method of steganographic transformation based on spatial domain modification of a rasterized container document. *Web Programming and Internet Technologies (WebConf2024): Proceedings of the 6th International Scientific and Practical Conference*, p. 337–340 (in Russian)
3. Ulasevich N. I., Zhilyak N. A. A steganographic method based on embedding additional elements under the colored areas in SVG format images. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2025, no. 2 (296), pp. 76–82. (In Russian).

Сведения об авторах

Уласевич Н.И. ассистент кафедры информационных систем и технологий. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», koliaulasevich@gmail.com

Савельева М.Г. ассистент кафедры информационных систем и технологий. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», saveleva@belstu.by

Information about the authors

Mikalai I. assistant of the Department of Information Systems and Technologies, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, koliaulasevich@gmail.com

Marina G. assistant of the Department of Information Systems and Technologies, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, saveleva@belstu.by

УДК 004.056.55

АКТУАЛЬНЫЕ ДОСТИЖЕНИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ В ОБЛАСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Сухоцкий

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь
РУП «Белэнергосетьпроект», г. Минск, Республика Беларусь*

Аннотация. В данной статье рассматриваются основные достижения в области криптографической защиты информации. Приводятся новые математические способы решения некоторых проблем контроля целостности.

Ключевые слова: достижения, контроль целостности, криптографическая защита информации.

CURRENT ADVANCES IN INTEGRITY CONTROL IN CRYPTOGRAPHIC INFORMATION PROTECTION

V.V. Sukhotski

*Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus
RUE “Belenergosetproekt”, Minsk, Republic of Belarus*

Abstract. This article examines key advances in cryptographic information protection. New mathematical methods for solving certain integrity control problems are presented.

Keywords: advances, integrity control, cryptographic information protection.

Введение

В настоящее время криптографические алгоритмы являются одним из основных способов защиты информации. Алгоритмы применяются для защиты информации при ее использовании и хранении на компьютерах, при передаче информации по сети. Данный способ защиты может гарантировать целостность, подлинность и/или конфиденциальность. Для каждой цели предназначены определенные алгоритмы. Алгоритмы шифрования используются для защиты конфиденциальности, алгоритмы формирования электронной цифровой подписи – для защиты целостности информации, алгоритмы идентификации – для проверки подлинности

источника данных. Из-за того, что методы нарушения конфиденциальности, целостности и подлинности информации часто меняются и число их растет, меняются требования к криптографическим алгоритмам и подходы к их использованию.

Основная часть

Использование таких разделов математики, как высшая алгебра и функциональный анализ, являются приоритетными в разработке криптографических алгоритмов для проверки целостности передаваемого сообщения. К одним из последних разработок относятся следующие:

1) код Рида-Соломона (недвоичный циклический код, позволяющий исправлять ошибки в блоках данных; изобретен в 1960 году сотрудниками лаборатории Линкольна Массачусетского технологического института Ирвингом Ридом и Густавом Соломоном);

2) правила построения геометрических кодов;

3) правила построения фрактала.

Первый алгоритм, используя средства высшей алгебры и функционального анализа, позволяет произвести проверку целостности информации и выявить ее нарушение, если таковое произошло. Алгоритм позволяет обрабатывать многомерные массивы.

При использовании второго алгоритма обнаружение и локализация ошибки в подблоках $m_1, m_2, \dots, m_k$ блока данных M обеспечиваются посредством вычисления системы значений хэш-функции (функция, отображающая блоки произвольного размера бит исходных данных в строки бит фиксированной длины) от совокупности подблоков данных, и ее сравнения с эталонной системой, при этом блок данных M для осуществления контроля целостности представляется в виде трехмерной матрицы. К данному блоку применяется хэш-функция по правилам построения геометрических кодов, при которых блоки данных, подлежащие защите, размещены в трехмерном кубе. Контроль целостности блока данных осуществляется путем сравнения значений хэш-функции, вычисленных при запросе на использование данных, подлежащих защите, и эталонных значений хэш-функции, вычисленных ранее.

В третьем алгоритме обнаружение и локализация данных с признаками нарушения целостности блока данных M , фрагментируемого на целевые блоки, расположенные на боковых ребрах треугольника, обеспечиваются посредством вычисления группы значений хэш-функции по правилам построения треугольника Паскаля и их сравнения с эталонными. Порядок вычисления значений хэш-функции и промежуточных результатов преобразований основан на правилах построения треугольника Паскаля, полученные значения размещают

в таблице, имеющей треугольную форму. По боковым сторонам полученного треугольника последовательно размещены промежуточные результаты преобразований, вычисляемые от блоков данных, подлежащих защите. На нижней стороне треугольника размещены блоки, предназначенные для обнаружения и локализации данных с признаками нарушения целостности. Блоки содержат значения хэш-функции h , для вычисления которых используются блоки данных, подлежащих защите, и результаты промежуточных преобразований нижнего уровня.

Заключение

Были изучены методы контроля целостности информации с применением разделов прикладной математики и линейной алгебры, которые позволяют более гибко настраивать криптографические алгоритмы для решения определенных проблем передачи информации. Данные методы характеризуются способностью локализовать подблоки данных с признаками нарушения целостности и сокращением избыточности вводимых контрольных данных.

Список использованных источников

1. Стариков Т.В., Сопин К.Ю., Диченко С.А., Самойленко Д.В., Сухов А.М., Брянцев А.В. и др. Способ контроля целостности многомерных массивов данных на основе правил построения кода Рида-Соломона // Google Patents. [Электронный ресурс]. – Режим доступа: <https://patentimages.storage.googleapis.com/75/87/45/f366e3b74d0b9d/RU2785862C1.pdf>
2. Диченко С.А., Самойленко Д.В., Финько О.А., Фадеев Р.В., Кись С.А., Брянцев А.В. и др. Способ контроля целостности данных на основе правил построения геометрических кодов // Google Patents. [Электронный ресурс]. – Режим доступа: <https://patentimages.storage.googleapis.com/a5/4f/25/f54e4dd4323c46/RU2758194C1.pdf>
3. Сопин К.Ю., Новиков П.А., Диченко С.А., Самойленко Д.В., Финько О.А. Способ криптографического контроля целостности данных на основе правил построения фракталов // Google Patents. [Электронный ресурс]. – Режим доступа: <https://patentimages.storage.googleapis.com/cf/5f/ac/06f89ada74cff0/RU2826863C1.pdf>

References

1. Starikov T.V., Sopin K.Y., Dichenko S.A., Samoylenko D.V., Sukhov A.M., Bryancev A.V., et al. Method for control of integrity of multimeric data arrays based on reed-solomon code building rules // Google Patents. [Electronic resource]. – Mode of access: <https://patentimages.storage.googleapis.com/75/87/45/f366e3b74d0b9d/RU2785862C1.pdf>
2. Dichenko S.A., Samoylenko D.V., Finko O.A., Fadeev R.V., Kis S.A., Bryancev A.V., et al. Method for monitoring data integrity based on the rules for constructing geometric codes // Google Patents. [Electronic resource]. – Mode of access: <https://patentimages.storage.googleapis.com/a5/4f/25/f54e4dd4323c46/RU2758194C1.pdf>
3. Sopin K.Y., Novikov P.A., Dichenko S.A., Samoylenko D.V., Finko O.A. Method for cryptographic data integrity control based on fractal construction rules // Google Patents.

[Electronic resource]. – Mode of access:
<https://patentimages.storage.googleapis.com/cf/5f/ac/06f89ada74cff0/RU2826863C1.pdf>.

Сведения об авторе

Сухоцкий В.В., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»; специалист, РУП «Белэнергосетьпроект», such998slava@outlook.com.

Information about the author

Sukhotski V.V., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics"; specialist, RUE "Belenergosityproekt", such998slava@outlook.com.

УДК 621.391

КОДИРОВАНИЕ АДРЕСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕЛИНЕЙНЫМ КОДОМ

А.И. Митюхин

*Институт информационных технологий учреждения образования
«Белорусский государственный университет информатики и
радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Рассматривается построение конструкции нелинейного бинарного кода для использования в качестве адресных слов, а также реализации начальной надежной синхронизации в радиосистемах с расширением спектра. Полученная система сигналов может использоваться для обеспечения помехоустойчивой передачи, процедуры распознавания адреса и защиты кодированной информации от перехвата. Ансамбль кодовых слов строится с использованием квадратичных вычетов по модулю простого числа и обладает криптографическими свойствами.

Ключевые слова: помехоустойчивость; спектр; радиосистема; корреляция; квадратичный вычет; ансамбль кодов; матрица Джекобстола.

ENCODING ADDRESS SEQUENCES WITH NONLINEAR CODE

A. Mitsiukhin

Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The construction of a nonlinear binary code for use as addressable codes, as well as the implementation of initial reliable synchronization in radio systems with spread spectrum, is considered. The resulting signal system can be used to ensure noise-free transmission, address recognition and protection of coded information from interception. The ensemble of codewords is built using quadratic deductions modulo prime and has cryptographic properties.

Keywords: noise immunity; spectrum; radio system; correlation; quadratic deduction; an ensemble of codes; Jacobsthal matrix.

Введение

Передача информации с использованием методов с расширением спектра позволяет обеспечить защиту от перехвата и воздействия организованных помех (глушение передачи) в плотно расположенных физических каналах тактического уровня. При этом особое внимание уделяется к выбору конструкций (n, M, d) -кодов с хорошими взаимно-корреляционными, спектральными и крипто характеристиками [1]. Основными критериями выбора параметров кода должны быть:

недопустимость предсказания закона формирования символов кодовой последовательности длиной n по правильно принятому сегменту слова длиной $k < n$;

значительная величина мощности M кода с заданным кодовым расстоянием d ;

желательно иметь код со свойствами ортогональности при вычисления взаимной корреляционной функции R (ВКФ) между входным процессом и копией сигнала [1].

законы кодирования кода должны эффективно меняться в сеансах связи;

период $T = n\tau$ (τ – длительности чипа слова) последовательности должен превышать длительность сеанса связи, т. е. отвечать свойству апериодичности.

На выбор кода для реальной радиосистемы влияет и такой системный аспект как синхронизация. Прием или декодирование информации становится возможным только после установления синхронизации по начальной фазе кодовой последовательности.

Теоретические принципы

Предметом статьи является обсуждение вопроса пригодности применения для передачи информации бинарного блочного нелинейного кода, построенного на основе использования квадратичных вычетов в конечном поле Галуа $GF(p^m)$, $m \in \mathbb{Z}^+$ и матриц Джекобстола размером $(p \times p)$. В сравнении с линейными кодами над расширенным полем $GF(2^m)$, $m \in \mathbb{Z}^+$ нелинейные конструкции кодов характеризуются значительно большей мощностью кода M и лучшими

криптографическими свойствами за счет негруппового свойства, т. е. не выполнения аксиомы замкнутости на множестве кода.

В обобщенном виде структура нелинейного квадратично вычетного кода порядком $n = p + 1$, определяется выражением

$$\mathbf{H} = \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1}^T & \mathbf{Q} - \mathbf{I} \end{pmatrix}, \quad (1)$$

где $\mathbf{I}$ – единичная матрица размером $p \times p$;

$\mathbf{1}$ – единичная строка размером $1 \times p$.

$\mathbf{Q} = (q_{ij})$ – матрица Джекобстола порядком $(p \times p)$.

Элементы матрицы $\mathbf{Q} = (q_{ij})$ определяются как

$$q_{ij} = \chi((j - i) \bmod p) = \chi\left(\frac{j - i}{p}\right), \quad (2)$$

где $\chi(i)$ – символ Лежандра.

В работе представлено построение кода на квадратичных вычетах в простом поле $GF(139)$ (1). Выбор значения $p = 139$ определялся параметром значности кода $n = p + 1$. Сравнение важнейших свойств полученного кода, удовлетворяющих требованиям приведенным выше, дано с известным линейным симплексным M -кодом

$$[n, k, d] = (2^m - 1, m, 2^{m-1}) = (127, 7, 64).$$

Основные теоретические и сравнительные экспериментальные результаты исследования приведены в таблице. Число ансамблей M -кода вычислено через функцию Эйлера числа n , $M = \varphi(n)/k = 126/7 = 18$. Число ансамблей нелинейного кода совпадает с длиной кода, что практически в 8 раз больше чем у линейного кода. Значения других параметров получены экспериментально, используя моделирование в среде MATLAB.

Свойства линейного и нелинейного кода
Properties of linear and nonlinear code

Конструкция кода	Блоковая длина кода n	Мощность кода M	Постоянная компонента кода $DC = -1/n$	Амплитудные коэффициенты ДПФ $ f_k $	ВКФ $\max R(\tau), \tau=0$
Линейный M -код	127	18	-0,0078	11,269 для $k = (1, \dots, 126)$.	-1; -17; 15
Нелинейный код	140	140	0	11,8 для $k = (1, \dots, 139)$.	0

В отличие от нулевой криптостойкости M -кода, криптостойкость кода на квадратичных вычетах зависит от знания числа p . Стандартные атаки становятся неэффективными из-за сложности нахождения формулы формирования (генерации) кода.

Заключение

Задача несанкционированного обнаружения нелинейного кода в сравнении с линейным M -кодом усложняется из-за использования ансамбля мощностью в 8 раз больше, а также отсутствием постоянной составляющей. В синхронном режиме и для кодового разделения каналов исследуемый нелинейный код имеет большую помехоустойчивость за счет идеальной ортогональности и может найти применение в радиосистемах с расширением спектра.

Список использованных источников / References

1. Mitsiukhin A. (2025) Detection and Analysis of Moving Objects. *International Journal on Applied Physics and Engineering*, Volume 4, 2025, 62–71.

Сведения об авторе

Митюхин А.И. Доцент, доцент, Институт информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», mityuhin@bsuir.by.

Information about the author

Mitsiukhin A. Associate Professor, Associate Professor, Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", mityuhin@bsuir.by.

УДК 004.056

МНОГОЭТАПНАЯ КОМПРОМЕТАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ: ВЗЛОМ ВЕБ-API И ГЕНЕРАТИВНАЯ ОБФУСКАЦИЯ ПОЛЕЗНОЙ НАГРУЗКИ

М.А. Винокуров, Д.А. Шумило

Учреждение образования «Гомельский Государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В статье исследуется комплексный сценарий современных кибератак, включающий этапы сетевого проникновения и исполнения вредоносного кода. Проанализированы недостатки стандартных модулей Metasploit Framework при обходе WAF и обосновано применение Python-скриптов для тестирования веб-API. Рассмотрен концептуально новый метод доставки полезной нагрузки после проникновения, основанный на генеративной обфускации с использованием локальных языковых моделей (LLM). Обоснована необходимость перехода от сигнатурного к поведенческому мониторингу на всех уровнях инфраструктуры.

Ключевые слова: веб-приложение; API; WAF; тестирование на проникновение; Metasploit Framework; обход защиты; генеративная обфускация; большая языковая модель; поведенческий анализ; информационная безопасность.

MULTISTAGE COMPROMISE OF INFORMATION SYSTEMS: WEB API HACKING AND GENERATIVE PAYLOAD OBFUSCATION

Vinokurov M., Shumilo D.

*Educational Institution “Francysk Skaryna Gomel State University”,
Gomel, Republic of Belarus*

Abstract. The article explores a complex scenario of modern cyberattacks, including the stages of network penetration and malicious code execution. The shortcomings of standard Metasploit Framework modules in bypassing WAF are analyzed, and the use of Python scripts for testing web APIs is justified. A conceptually new method of payload delivery after penetration, based on generative obfuscation using local large language models (LLMs), is considered. The necessity of transitioning from signature-based to behavioral monitoring at all infrastructure levels is substantiated.

Keywords: web application; API; WAF; penetration testing; Metasploit Framework; defense bypass; generative obfuscation; large language model; behavioral analysis; information security.

Введение

Современные информационные системы сталкиваются с угрозами, реализующими многовекторный подход к обходу защиты. Эффективная кибератака сегодня – это не единичное действие, а строго выверенная цепочка, где злоумышленникам необходимо преодолеть как минимум два рубежа: сетевой периметр и средства защиты конечных точек. В условиях стремительного развития защитных механизмов киберпреступники вынуждены непрерывно совершенствовать тактики скрытного

присутствия. Это приводит к формированию комплексных сценариев компрометации, где на каждом шаге применяются специфические, зачастую неочевидные методы уклонения от мониторинга. Наибольшую опасность в таких сценариях представляют комбинированные техники, эксплуатирующие уязвимости программных интерфейсов (API) для первичного сетевого доступа, с последующим применением алгоритмов машинного обучения для маскировки исполнения вредоносного кода непосредственно внутри атакованной инфраструктуры.

Основная часть

В современной микросервисной архитектуре основным вектором начального доступа выступают веб-API. Злоумышленники активно используют методы автоматизированного перебора, однако классический брутфорс оперативно блокируется межсетевыми экранами уровня приложений. Современные системы защиты анализируют не только частоту запросов, но и цифровые отпечатки протокола TLS (JA3/JA3S), а также поведенческие паттерны.

Проведение качественного аудита безопасности в таких условиях требует адекватного инструментария. Практика показывает, что стандартные средства тестирования на проникновение, включая многие базовые модули платформы Metasploit Framework, демонстрируют недостаточную гибкость. Они обладают жесткой архитектурой отправки запросов и легко детектируются по характерным сетевым сигнатурам. Для успешной эмуляции современных атак требуется разработка кастомного инструментария. В частности, встроенные сканеры испытывают критические сложности с фаззингом многоуровневых JSON-объектов и запросов GraphQL, что делает практически невозможным поиск уязвимостей нарушения авторизации на уровне свойств объектов.

Разработка специализированных модулей на языке Python для среды Metasploit позволяет решить эту проблему за счет реализации интеллектуального парсинга ответов API и автоматического извлечения, и обновления JWT-токенов «на лету». Кроме того, применение асинхронных Python-библиотек дает возможность генерировать распределенный сетевой трафик через пулы резидентных прокси. Это обеспечивает надежный обход алгоритмов, используемых современными API-шлюзами для динамического ограничения запросов, не вызывая подозрений у аналитических систем WAF.

После успешного проникновения через API (например, получения RCE-уязвимости или доступа с правами администратора) перед атакующим встает задача скрытной доставки полезной нагрузки. На этом этапе классические методы обфускации (упаковщики, шифровальщики) теряют эффективность: зашифрованный файл обладает аномально высокой

энтропией, что моментально выявляется современными ML-детекторами антивирусных систем.

Решением для злоумышленников стало использование больших языковых моделей. Новый подход отказывается от сокрытия уже написанного вредоносного кода – вместо этого ИИ синтезирует его непосредственно на атакованном узле. Схема атаки выглядит следующим образом: через уязвимый API на сервер загружается легитимная, на первый взгляд, программа-загрузчик, содержащая штатные библиотеки для работы с машинным обучением (например, `onnxruntime.dll`) и файл с весами локальной нейросети. Статические сканеры не видят в этом наборе угрозы. В момент запуска загрузчик собирает телеметрию системы (версию ОС, открытые порты, установленные утилиты) и передает их в качестве инструкции нейросети. В свою очередь, языковая модель, предварительно дообученная злоумышленниками на генерацию эксплойтов, синтезирует уникальный вредоносный код прямо в оперативной памяти.

В результате вредоносная логика скрывается не в зашифрованном архиве, а в миллиардах числовых параметров (весах) матриц модели ИИ. Процесс дообучения становится высшей формой обфускации. Извлечь вредоносную сигнатуру из матриц весов статическим анализом технически невозможно – это абсолютный черный ящик.

Заключение

Таким образом, современные атаки на веб-приложения характеризуются глубокой маскировкой на каждом этапе своего жизненного цикла. На уровне сети (при атаке на API) применение гибких скриптов на Python позволяет злоумышленникам обходить WAF, полностью имитируя поведение легитимных клиентов. На уровне хоста (при исполнении полезной нагрузки) использование дообученных языковых моделей сводит на нет эффективность антивирусных сканеров, маскируя вирус под легитимные процессы машинного обучения.

Анализ этих векторов доказывает, что парадигма статической защиты окончательно устарела. Обеспечение безопасности требует концептуального перехода к динамическому контролю инфраструктуры. Эффективная защита возможна только путем непрерывного поведенческого мониторинга: выявления нетипичной последовательности вызовов API на сетевом шлюзе, а также блокировки бесфайлового исполнения кода и аномальных пиков потребления вычислительных ресурсов (CPU/GPU) на конечных узлах.

Сведения об авторах

Винокуров М.А., студент 4-го курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования

«Гомельский государственный университет имени Франциска Скорины», maks_vinokurov_2005@mail.ru.

Шумило Д.А., студент 4-го курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», shmain125@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиопизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Vinokurov M., 4th year student of the Faculty of Physics and Information Technology specialty "Computer security", Educational Institution "Francysk Skaryna Gomel State University", maks_vinokurov_2005@mail.ru.

Shumilo D., 4th year student of the Faculty of Physics and Information Technology specialty "Computer security", Educational Institution "Francysk Skaryna Gomel State University", shmain125@gmail.com.

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Educational Institution "Francysk Skaryna Gomel State University", vaskevich@gsu.by.

УДК 538.9

ВЛИЯНИЕ ПОДЛОЖКИ НА КОРРЕЛЯЦИОННЫЕ ФУНКЦИИ ОСЕЙ СЛУЧАЙНОЙ АНИЗОТРОПИИ В МАССИВАХ НАНОЧАСТИЦ Co/CoO

Е.С. Назаренко, А.Л. Данилюк

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Методом интегрального преобразования Мейера проведен сравнительный анализ корреляционных функций осей случайной анизотропии для двумерных массивов наночастиц Co/CoO (ядро/оболочка) на подложках меди (Cu) и медь/графен (Cu/G). Показано, что тип подложки определяет качественный вид корреляционной функции: для Co/CoO/Cu характерны осциллирующие дальнедействующие корреляции, для Co/CoO/Cu/G – монотонные, немонотонные и скачкообразные зависимости.

Ключевые слова: случайная анизотропия, корреляционная функция, преобразование Мейера, наночастицы Co/CoO, графен.

INFLUENCE OF THE SUBSTRATE ON THE CORRELATION FUNCTIONS OF RANDOM ANISOTROPY AXES IN ARRAYS OF Co/CoO NANOPARTICLES

K.S. Nazarenka, A.L. Danilyuk

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. A comparative analysis of the correlation functions of random anisotropy axes for two-dimensional arrays of Co/CoO nanoparticles (core/shell) on copper (Cu) and copper/graphene (Cu/G) substrates was performed using the Meyer integral transform method. It was shown that the substrate type determines the qualitative form of the correlation function: Co/CoO/Cu are characterized by oscillating long-range correlations, while Co/CoO/Cu/G exhibits monotonic, non-monotonic, and jump-like dependencies.

Keywords: random anisotropy, correlation function, Meyer transform, Co/CoO nanoparticles, graphene.

Введение

Массивы ферромагнитных наночастиц на поверхности твердых тел перспективны для спинтроники. Классическая модель случайной анизотропии (RAM) использует только экспоненциальную корреляционную функцию. Подход на основе интегрального преобразования Мейера [1] позволяет определять реальный вид корреляционных функций $C(z)$ из экспериментальных данных. В работе этот подход применен для сравнения двух типов подложек.

Основная часть

Закон приближения к намагниченности насыщения для двумерной магнитной системы имеет вид интегрального преобразования Мейера (K-transform) [1]

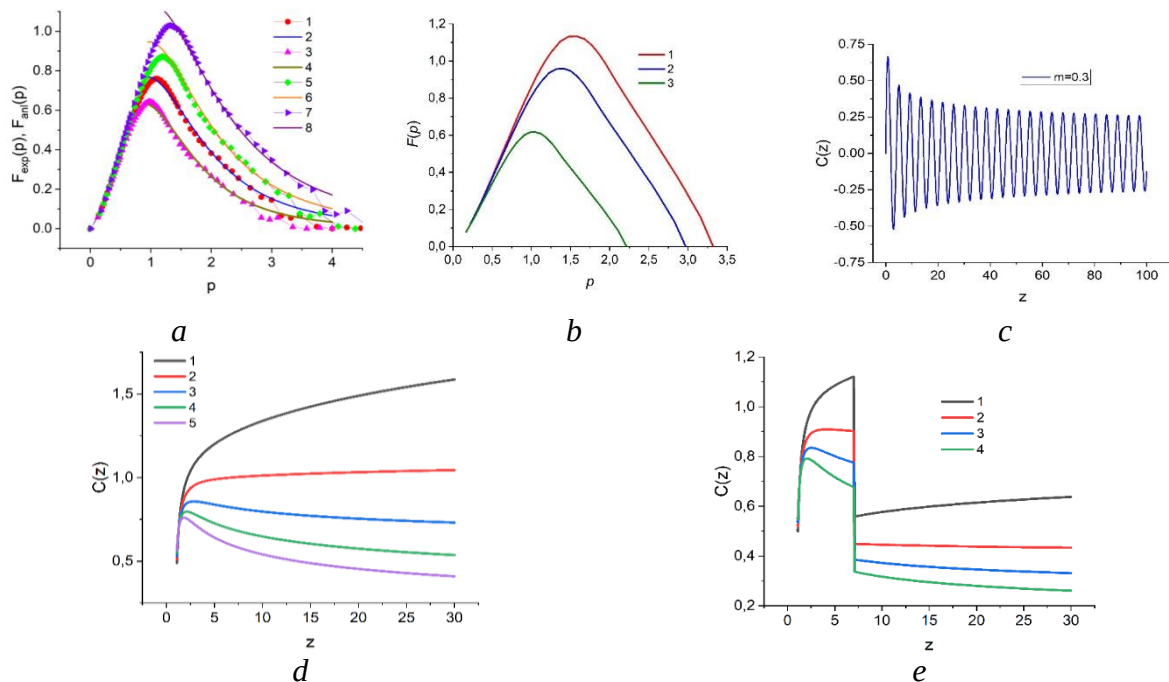
$$F(p) = \frac{32p^{\frac{3}{2}}}{4\pi} \left(\frac{H_{ex}}{H_a} \right)^2 \frac{\delta M(p)}{M_s} = \int_0^\infty z^{\frac{3}{2}} C(z) \sqrt{pz} K_1(pz) dz, \quad (1)$$

где $p = \left(\frac{H}{H_{ex}} \right)^{1/2}$, $\delta M(p) = M_s - M(H)$, H_{ex} – поле обмена, H_a – поле случайной анизотропии, K_1 – модифицированная функция Бесселя второго рода первого порядка.

Функция-образ $F(p)$ получается из экспериментальных петель гистерезиса, а корреляционная функция $C(z)$ находится путем обратного преобразования Мейера.

Рисунок представляет сопоставление функций-образов $F(p)$ для обеих систем при $T=4$ К. Для Co/CoO/Cu характерна вогнутость спадающего участка, для Co/CoO/Cu/G спад имеет практически линейный характер.

Рисунок демонстрирует корреляционные функции $C(z)$ для Co/CoO/Cu/G. В зависимости от параметра μ функция $C(z)$ может быть монотонной, выходить на насыщение или иметь немонотонный характер с максимумом (рис. 2a) или приобретать при критических параметрах μ скачкообразный характер (рис. 2b), что связано с самоорганизацией наночастиц в кластеры.



Функции-образы $F(p)$ при $T=4$ К для различных значений H_{ex} и корреляционная функция $C(z)$ для Co/CoO/Cu (c): a – для Co/CoO/Cu ; b – для Co/CoO/Cu/G ,

Корреляционные функции $C(z)$ при $d=1,0$: d – $\mu=-0,833$ (1), $\mu=-0,77$ (2), $\mu=-0,714$ (3), $\mu=-0,67$ (4), $\mu=-0,625$ (5); e – $\mu=-0,8$ (1), $\mu=-0,74$ (2), $\mu=-0,7$ (3), $\mu=-0,662$ (4)

В системе Co/CoO/Cu высокопроводящая медная подложка обеспечивает значительный вклад косвенного обменного взаимодействия (РККИ) [2]. Осциллирующий и слабозатухающий характер корреляционной функции связан с конкуренцией этого взаимодействия с локальными эффектами: сильной магнитной анизотропией оболочки CoO ($K \sim 10^7$ Дж/м³) и обменным смещением на границе Co/CoO . Эти факторы «закрепляют» оси анизотропии ядер Co , поддерживая корреляции на больших расстояниях.

В системе Co/CoO/Cu/G слой графена ослабляет вклад РККИ из-за меньшей концентрации носителей заряда [2]. Доминирующими становятся дипольное взаимодействие и флуктуации случайной анизотропии, что приводит к разнообразному поведению $C(z)$. При повышении температуры до 25 К функция-образ для Co/CoO/Cu/G приобретает вогнутость [2], сближаясь с поведением системы на чистой меди.

Заключение

Проведенный сравнительный анализ показал, что интегральный подход на основе преобразования Мейера позволяет выявлять качественные различия в корреляционных функциях осей случайной анизотропии. Тип подложки является ключевым фактором, определяющим характер корреляций: на меди –дальнодействующие осциллирующие

корреляции, на графене/меди – монотонные, немонотонные и скачкообразные зависимости. Полученные результаты важны для управления магнитными свойствами композитов при разработке спинтронных устройств.

Список использованных источников

1. Chudnovsky E.M., Fernandez-Bac J.A., Ching W.-Y. (1995) The magnetism of amorphous metals and alloys. *World Scientific*. Singapore. Ch. 3, 143–175.
2. Danilyuk A.L., Nazarenka E.S., Vorobyova S.A., Fedotova J.A., Prischepa S.L. (2023) Low-temperature magnetic ordering in Co core/CoO shell nanoparticles on the copper surface. *Current Applied Physics*. Vol. 56, 79–84.

References

1. Chudnovsky E.M., Fernandez-Bac J.A., Ching W.-Y. (1995) The magnetism of amorphous metals and alloys. *World Scientific*. Singapore. Ch. 3, 143–175.
2. Danilyuk A.L., Nazarenka E.S., Vorobyova S.A., Fedotova J.A., Prischepa S.L. (2023) Low-temperature magnetic ordering in Co core/CoO shell nanoparticles on the copper surface. *Current Applied Physics*. Vol. 56, 79–84.

Сведения об авторах

Назаренко Е.С., аспирант кафедры микро- и нанoeлектроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», katanaz2001@gmail.com.

Данилюк А.Л., к.ф.-м.н., доцент, доцент кафедры микро- и нанoeлектроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danilyuk@bsuir.by.

Information about the authors

Nazarenka K.S., postgraduate student at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, katanaz2001@gmail.com.

Danilyuk A.L., Cand. of Sci., Associate Professor, Associate Professor at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, danilyuk@bsuir.by.

УДК 004.056

ТЕХНОЛОГИЯ АВТОМАТИЗИРОВАННОГО ФОРМИРОВАНИЯ БАЗЫ ЛЕГИТИМНЫХ TLS-ОТПЕЧАТКОВ

Д.И. Неслуховский, Д.С. Горин

МИРЭА – Российский технологический университет, г. Москва, Россия

Аннотация. В работе рассматривается технология автоматизированного формирования базы легитимных клиентских TLS-отпечатков на основе контролируемого воспроизведения сетевых сессий в изолированном периметре. Описываются этапы

подготовки окружений, запуска клиентских приложений, захвата трафика и извлечения клиентских отпечатков из сообщений ClientHello для дальнейшего использования в системах мониторинга и защиты информации.

Ключевые слова: TLS fingerprinting; идентификация сетевого трафика; цифровые отпечатки; база отпечатков; мониторинг трафика; обнаружение аномалий.

TECHNOLOGY FOR AUTOMATED CONSTRUCTION OF A DATABASE OF LEGITIMATE CLIENT TLS FINGERPRINTS

D.I. Neslukhovskiy, D.S. Gorin

MIREA – Russian Technological University, Moscow, Russia

Abstract. The paper presents a technology for automated construction of a database of legitimate client TLS fingerprints based on controlled replay of network sessions in an isolated environment. The approach covers environment preparation, client application deployment, traffic capture, and extraction of client fingerprints from ClientHello messages for subsequent use in traffic monitoring and information security systems.

Keywords: TLS fingerprinting; network traffic identification; digital fingerprints; fingerprint database; traffic monitoring; anomaly detection.

Введение

Идентификация сетевого трафика является важным этапом защиты информации и организации пассивного мониторинга, поскольку позволяет устанавливать соответствие между наблюдаемыми соединениями и типами используемого клиентского программного обеспечения (ПО), включая веб-браузеры, мессенджеры, почтовые клиенты и иные сетевые приложения. Существенная доля трафика в современных сетях защищается с использованием протокола Transport Layer Security (TLS), что делает особенно востребованными методы, не требующие расшифрования содержимого сеанса и опирающиеся на анализ служебных параметров протокольного взаимодействия.

Одним из практичных подходов к идентификации зашифрованного трафика является набор методов, в совокупности именуемых «TLS fingerprinting», при которых цифровые отпечатки (ЦО, англ. fingerprints) формируются по совокупности параметров установления и ведения защищенного соединения, в первую очередь по структуре и содержимому сообщения ClientHello, и тем самым отражают устойчивые особенности конкретных реализаций клиентских приложений [1].

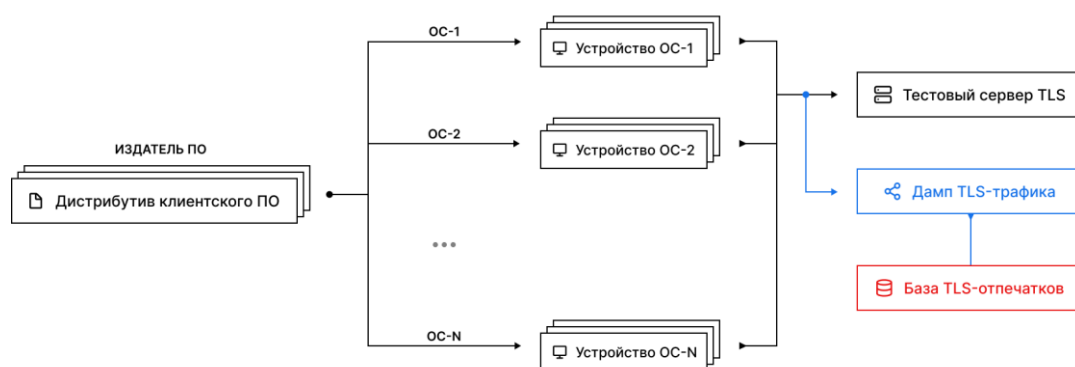
Как показано в работе [2], по мере выхода новых версий прикладного ПО пространство используемых протокольных признаков постоянно расширяется, в конфигурациях клиентов появляются ранее не встречавшиеся элементы, что приводит к быстрому устареванию статичных наборов эталонных профилей. Это обуславливает необходимость поддерживать базу легитимных клиентских отпечатков, формирующих набор эталонных профилей, как регулярно

и верифицируемо пополняемый ресурс, учитывающий эволюцию конфигураций реальных клиентов.

Основная часть

Постановка задачи. В работе рассматриваются организационные и технические вопросы получения исходных данных для методов идентификации клиентов по их ЦО в TLS-соединениях. Целью является проектирование поэтапного процесса автоматизированного формирования базы легитимных клиентских отпечатков, независимого от конкретных алгоритмов их последующего анализа. Предполагается, что процесс должен, используя только верифицированные экземпляры клиентского ПО и контролируемый тестовый периметр, автоматически собирать и разворачивать требуемые версии приложений, инициировать характерные для них сетевые сценарии, регистрировать результирующий трафик и извлекать из него клиентские ЦО в структурированном виде. Дополнительными требованиями являются масштабируемость по числу поддерживаемых клиентов и окружений, а также пригодность к регулярному повторному запуску по мере выхода новых версий программного обеспечения.

Методика формирования базы. Общая структура предлагаемого процесса формирования базы легитимных ЦО представлена на схеме и включает последовательные стадии от подготовки экземпляров клиентского ПО до аккумуляции результатов в базе данных.



Структура процесса формирования базы клиентских TLS-отпечатков
Structure of the client TLS fingerprint database generation process

На этапе подготовки окружений выполняется систематический сбор экземпляров клиентского ПО: с официальных ресурсов издателей ПО загружаются установочные пакеты, образы и другие дистрибутивные формы актуальных и архивных версий, после чего они разворачиваются на изолированных тестовых стендах с различными сочетаниями операционных систем и аппаратных платформ. Это обеспечивает

однозначную идентификацию исходной конфигурации и позволяет учитывать влияние программно-аппаратного окружения на формируемые клиентские TLS-отпечатки.

Далее развернутые экземпляры клиентского ПО в автоматизированном режиме выполняют заранее заданные сценарии взаимодействия с целевой (тестовой) серверной инфраструктурой в закрытом сетевом контуре, свободном от посторонних источников трафика; сценарии моделируют типичные для соответствующих классов приложений действия пользователя, что позволяет получать ЦО в условиях, приближенных к реальной эксплуатации.

Сетевая активность в пределах выделенного контура регистрируется на серверной стороне и сохраняется в виде дампов трафика в исходном виде для последующего анализа. В рамках автоматизированной обработки дампов выделяются соединения, инициированные тестируемыми клиентами, и извлекаются релевантные протокольные параметры, в первую очередь поля сообщения ClientHello (версии протокола, наборы шифров, расширения и связанные параметры), на основе которых формируются один или несколько клиентских ЦО на соединение. Полученные отпечатки вместе с метаданными (тип приложения, версия и конфигурация, операционная система, аппаратная платформа, дата и условия сбора и др.) заносятся в итоговую базу данных. Такая организация процесса упрощает его регулярный перезапуск и масштабирование при расширении перечня поддерживаемых приложений и платформ.

Практическое применение. Сформированная таким образом база легитимных клиентских ЦО может использоваться в системах мониторинга и обнаружения аномалий для сопоставления наблюдаемых клиентских отпечатков, вычисляемых по сообщениям ClientHello, с эталонными профилями и выделения соединений, инициируемых неизвестными либо подозрительными конфигурациями клиентского ПО. В системах фильтрации и контроля доступа такая база служит дополнительным источником признаков для проверки согласованности прикладных атрибутов (таких как заявленный тип или версия клиента) с фактической конфигурацией его TLS-стека [3]. Также, в задачах противодействия автоматизированным злоупотреблениям и вторжению в инфраструктуру наличие актуальных профилей легитимных клиентов облегчает выявление ClientHello, сформированных типовыми сетевыми стеками общего назначения (например, встроенными реализациями в средах выполнения JavaScript или Python), конфигурация которых заметно отличается от характерных для реальных пользовательских приложений.

Заключение

Идентификация клиентов по их ЦО представляет собой важный инструмент анализа зашифрованного трафика. Для надежного применения этого инструмента недостаточно одних алгоритмов вычисления ЦО, также критически важен и конвейер, который в контролируемых условиях формирует достоверные клиентские профили и обеспечивает их регулярное обновление с учетом дрейфа признаков и появления новых конфигураций. Описанный процесс автоматического формирования базы легитимных клиентских отпечатков, основанный на воспроизведении типичных сетевых сценариев и последующей обработке трафика в контролируемом периметре, решает эту задачу и создает основу для интеграции методов TLS fingerprinting в прикладные системы мониторинга и защиты информации.

Список использованных источников

1. Husak M., Cermak M., Jirsik T., Celeda P. (2015) Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. *10th International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24-27 August, 2015*. 389–396. DOI 10.1109/ARES.2015.35.
2. Неслуховский Д.И., Нефедов В.С. (2025) Оценка расширения пространства признаков TLS-отпечатков веб-браузеров во времени. *Кибернетика и информационная безопасность «КИБ-2025» : Сборник научных трудов Третьей Всероссийской научно-технической конференции: в 2-х томах, Москва, 3-4 декабря 2025 года*. Москва, НИЯУ МИФИ. 2. 70–71. EDN RVUAYZ.
3. Heino J., Hakkala A., Virtanen S. (2023) Categorizing TLS traffic based on JA3 pre-hash values. *Procedia Computer Science*. 220 (2023). 94–101. DOI 10.1016/j.procs.2023.03.015.

References

1. Husak M., Cermak M., Jirsik T., Celeda P. (2015) Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. *10th International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24-27 August, 2015*. 389–396. DOI 10.1109/ARES.2015.35.
2. Neslukhowsky D.I., Nefedov V.S. (2025) Evaluation of the Expansion of the Feature Space of TLS Fingerprints of Web Browsers Over Time. *Cybernetics and Information Security «KIB-2025» : Proceedings of the Third All-Russian Scientific and Technical Conference, in 2 Volumes, Moscow, December 3–4, 2025*. Moscow, MEPhI. 2. 70–71. EDN RVUAYZ.
3. Heino J., Hakkala A., Virtanen S. (2023) Categorizing TLS traffic based on JA3 pre-hash values. *Procedia Computer Science*. 220 (2023). 94–101. DOI 10.1016/j.procs.2023.03.015.

Сведения об авторах

Неслуховский Д.И., студент каф. КБ-2 «Информационно-аналитические системы кибербезопасности», Институт кибербезопасности и цифровых технологий,

федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», neslukhovskiy.d@yandex.ru.

Горин Д.С., канд. экон. наук., доцент, зав. каф. КБ-3 «Разработка программных решений и системное программирование», Институт кибербезопасности и цифровых технологий, федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», gorin@mirea.ru.

Information about the authors

Neslukhovskiy D.I., Student of Department KB-2 «Informational and Analytical Cybersecurity», Institute of Cybersecurity and Digital Technologies, Federal State-Funded Educational Institution of Higher Education «MIREA – Russian Technological University», neslukhovskiy.d@yandex.ru.

Gorin D.S., Cand. Econ. Sci., Associate Professor, Head of the Department KB-3 «Software Development and Systems Programming», Institute of Cybersecurity and Digital Technologies, Federal State-Funded Educational Institution of Higher Education «MIREA – Russian Technological University», gorin@mirea.ru.

УДК 004.056:004.434

АКТИВНАЯ ЗАЩИТА ИСПОЛНЯЕМОГО КОДА С ИСПОЛЬЗОВАНИЕМ АППАРАТНЫХ КРИПТОСРЕДСТВ И ПОЛИМОРФНЫХ КЛАССОВ C++

Н.В. Хаджинова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассматривается подход к активной защите исполняемого кода, интегрирующий механизмы объектно-ориентированного программирования с аппаратными криптосредствами (TPM, HSM). Предлагается архитектура, где критический компонент представлен полиморфным классом, инкапсулирующим функциональную логику и контекст безопасности. Математически описана процедура верификации целостности в реальном времени. Аппаратные средства обеспечивают корень доверия. Накладные расходы составляют 8–12 %, что приемлемо для распределенных систем управления.

Ключевые слова: активная защита кода; полиморфные классы; аппаратные криптосредства; TPM; контроль целостности.

ACTIVE PROTECTION OF EXECUTABLE CODE USING HARDWARE CRYPTOGRAPHIC MEANS AND POLYMORPHIC C++ CLASSES

N.V. Khajynava

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. An approach to active protection of executable code integrating object-oriented programming with hardware cryptographic means (*TPM*, *HSM*) is considered. An architecture is proposed where each critical component is represented by a polymorphic class encapsulating functional logic and security context. The real-time integrity verification procedure is mathematically described. Hardware tools provide a root of trust. Overhead costs are 8–12 %, which is acceptable for distributed control systems.

Keywords: active code protection; polymorphic classes; hardware cryptographic means; *TPM*; integrity control.

Введение

Программные системы функционируют в условиях постоянных атак на исполняемый код: модификация, внедрение вредоносных компонентов, нарушение потока выполнения. Особую опасность представляют атаки времени выполнения (эксплуатация уязвимостей памяти, подмена управления). Традиционные методы защиты (статический анализ, стандартный контроль целостности) не всегда оперативно реагируют на динамические угрозы в средах с высокими требованиями к детерминированности.

Основная часть

Предлагаемый подход основан на представлении каждого критического компонента полиморфным классом, наследующим от абстрактного базового класса *SecureComponent* (рисунок 1). Это позволяет оптимизировать распределение ресурсов и инкапсулировать механизмы защиты. При создании экземпляра (в конструкторе) иницируется аттестация:

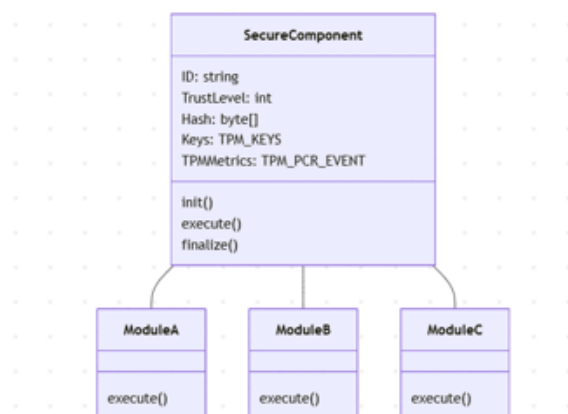
- вычисление текущего хеша сегмента кода класса;
- сравнение с эталонным «слепок», хранящимся в защищенной памяти (на сервере аттестации или в хранилище, ассоциированном с *TPM*);
- проверка регистров конфигурации платформы (*PCR*) для подтверждения доверенной среды загрузки.

Аппаратные криптосредства (*HSM/TPM 2.0*) хранят долгоживущие ключи дешифрования [1]. Код может находиться в памяти в зашифрованном виде и расшифровываться *just-in-time* перед вызовом виртуальной функции через *vtable*, которая также мониторится.

На рисунке показана иерархия: базовый класс *SecureComponent* содержит чисто виртуальные методы и защищенные члены для контекста безопасности. Производные классы переопределяют методы и наследуют механизмы верификации, вызываемые в конструкторе и деструкторе.

Создание объекта разрешается только при условии $E(C_i) = 1$. В случае нарушения целостности или несоответствия платформенного контекста

срабатывает механизм экстренного завершения процесса с очисткой данных в деструкторах.



Наследование от абстрактного класса
Inheritance from an abstract class

Процесс верификации компонента C_i при его активации в системе можно представить в виде функции доверия $E(C_i)$:

$$E(C_i) = \Phi(H(P_i) \oplus PCR_j, \sigma_{HSM}), \quad (1)$$

где $H(P_i)$ – хеш-сумма сегмента памяти, занимаемого кодом класса; PCR_j – значение регистра конфигурации платформы *TPM*; σ_{HSM} – эталонная цифровая подпись, вычисленная для корректного состояния компонента и защищенная аппаратным модулем; Φ – функция проверки, выполняемая в защищенном контуре аппаратного модуля (например, *TPM* или *HSM*).

Интеграция с аппаратными средствами позволяет минимизировать временные затраты на криптографические операции. Суммарное время выполнения защищенного вызова T_{total} определяется как:

$$T_{total} = T_{exec} + T_{verify} + T_{decrypt}, \quad (2)$$

где T_{verify} – время, затрачиваемое на вычисление хеша процессором и его верификацию с эталонным значением, защищенным *TPM* [2]. T_{bxc} – время выполнения самой защищаемой функции. Для сегментов кода размером до 1 МБ операция верификации на процессорах среднего класса (например, *Intel Core i5-10600KF* на частоте 3,5 ГГц) не превышает 1,5 мс.

Для оценки применимости подхода проведен эксперимент на прототипе системы управления сетевыми ресурсами. Конфигурация: *Intel Core i5-10600KF*, 16 ГБ RAM, *TPM 2.0*, *Linux (kernel 5.x)* с поддержкой измеряемой загрузки. Тестовое приложение включало 10 компонентов – полиморфных классов C++, наследующих от *SecureComponent*.

Оценивалось влияние защиты на время отклика (*latency*). Базовый уровень – проверка целостности кода при инициализации (SHA-256,

эталонные значения в TPM). Средний уровень – контроль целостности потока выполнения при вызове виртуальных методов. Полный уровень – динамическое шифрование сегментов кода с ключами, привязанными к состоянию платформы.

Тесты (не менее 30 замеров на режим) показали: накладные расходы CPU составляют 3–5 % для базовой верификации и до 12 % при полном шифровании.

Заключение

Предложенный подход обеспечивает интеграцию механизмов безопасности в архитектуру ПО за счет сочетания полиморфных абстракций C++ и аппаратных криптосредств. Экспериментально подтверждены практическая применимость и приемлемость накладных расходов (8–12 % в полном режиме). Дальнейшее развитие связано с расширением защиты для распределенных систем и автоматизацией контроля доверенного состояния.

Список использованных источников

1. Субашины С., Кавита В. (2011) Обзор проблем безопасности в моделях предоставления облачных вычислений. Journal of Network and Computer Applications, 34 (1), 1–11.
2. Артур У., Челленер Д., Гольдман К. (2014) Практическое руководство по TPM 2.0: Использование TPM в новой эре безопасности. Syngress.

References

1. Subashini S., Kavitha V. (2011) A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications, 34 (1), 1–11 (in Russian).
2. Arthur W., Challener D., Goldman K. (2014) A Practical Guide to TPM 2.0: Using the TPM in the New Age of Security. Syngress.

Сведения об авторе

Хаджинова Наталья Владимировна, старший преподаватель кафедры ИТАС, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», khajynova@bsuir.by.

Information about the author

Khajynava, N., Senior Lecturer at the Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", khajynova@bsuir.by.

УДК 004.056:004.942

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМОВ АКТИВНОЙ ЗАЩИТЫ В РАСПРЕДЕЛЕННЫХ МУЛЬТИАГЕНТНЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Н.В. Хаджинова

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. Предложена многоуровневая схема активной защиты распределенных мультиагентных систем управления, объединяющая контроль целостности кода, мониторинг контекста агентов и детектирование аномалий. Схема базируется на объектно-ориентированных полиморфных сетях Петри (PPN), позволяющих встраивать процедуры защиты в архитектуру интерпретаторов без нарушения требований реального времени. Экспериментальная оценка показала накладные расходы 8–12 % при точности обнаружения аномалий до 96 %, что соответствует требованиям систем мягкого реального времени.

Ключевые слова: активная защита; мультиагентные системы; распределенные системы управления; целостность; контроль контекста; детектирование аномалий; сети Петри; полиморфизм; безопасность в реальном времени; киберфизические системы.

USING ACTIVE PROTECTION MECHANISMS IN DISTRIBUTED MULTI-AGENT CONTROL SYSTEMS

N.V. Khajynava

*Educational Institution “Belarusian State University of Informatics and
Radioelectronics”, Minsk, Republic of Belarus*

Abstract. A multi-level active protection scheme for distributed multi-agent control systems is proposed, combining code integrity control, agent context monitoring, and anomaly detection. The scheme is based on object-oriented polymorphic Petri nets (PPN), which allow embedding protection procedures into the interpreter architecture without violating real-time requirements. Experimental evaluation showed an overhead of 8–12 % with an anomaly detection accuracy of up to 96 %, meeting the requirements of soft real-time systems.

Keywords: active protection; multi-agent systems; distributed control systems; integrity; context control; anomaly detection; Petri nets; polymorphism; real-time security; cyber-physical systems.

Введение

Распределенные мультиагентные системы (МАС) широко применяются в киберфизических системах и промышленном интернете вещей (IIoT). Децентрализация создает дополнительные векторы угроз: состязательные атаки, компрометация кода, подмена сообщений [1]. Традиционные методы защиты (антивирусы, статический анализ) недостаточно эффективны в реальном времени, где критична предсказуемость реакции. Предлагается встраиваемая в интерпретаторы

архитектура активной защиты на основе полиморфных расширений сетей Петри [2].

Основная часть

Схема включает четыре уровня контроля, встроенных в интерпретатор PPN:

Code-time – верификация кода (SHA-256, цифровые подписи). Эталонные хеши хранятся в TPM; при модификации модуль не исполняется.

Load-time – доверенная загрузка (*Trusted Boot*): каждый этап инициализации расширяет PCR TPM, гарантируя старт из доверенного состояния.

Runtime – мониторинг контекста агента (процесс, права, файлы, сеть) и контроль потока управления (CFI). Изоляция через песочницу (seccomp).

Anomaly Detection – по профилям нормального поведения выявляются отклонения; при обнаружении агент изолируется.

Защита встраивается через класс *SecureTransition*, наследующий базовый полиморфный переход *Transition<Time>*. Виртуальные методы *E*, *C*, *D*, *F* дополнены вызовами процедур безопасности. Метод *E* отвечает за проверку возможности срабатывания перехода, *C* – за изъятие токенов из входных позиций, *D* – за вычисление задержки, *F* – за генерацию выходных токенов.

```
template <class Time>
struct SecureTransition : public Transition<Time> {
    MultilevelSecurityProtection<Time> securityStack;
    ExecutionContextMonitor<Time> contextMonitor;
    virtual int E(int index) override {
        if (!securityStack.verifyFullSecurityStack()) return 0;
        if (!contextMonitor.E(index)) return 0;
        return 1;
    }
    virtual void C(int index) override {
        contextMonitor.C(index); // фиксация контекста перед выполнением
        consumeTokens();
    }
    virtual Time D(int index) override {
        return estimateExecutionTime() + securityStack.getOverhead() + contextMonitor.D(index);
    }
    virtual void F(int index) override {
        if (!contextMonitor.validateContextIntegrity(index)) {
            recordSecurityEvent("CONTEXT_COMPROMISE");
            isolateAgent();
            return;
        }
        generateTokens();
    }
};
```

Такой подход обеспечивает встраивание проверок в декларативную структуру модели, сохраняя ее формальную семантику. Для минимизации накладных расходов захват контекста выполняется легковесными системными вызовами с кэшированием; для критических переходов допускается выборочный контроль.

Эксперименты проведены на стенде: процессор Intel Core i5-10600KF, 16 ГБ оперативной памяти, модуль TPM 2.0, ОС на базе ядра Linux (kernel 5.x). МАС включала от 10 до 100 агентов, взаимодействующих по протоколам аукциона и консенсуса. Моделировались атаки: модификация кода, подмена сообщений, переполнение буфера. Результаты (50 запусков) приведены в таблице. Архитектура Intel Core i5 обеспечивает детектирование аномалий в пределах 15 мс, что делает схему применимой в системах с циклом управления менее 20 мс.

Накладные расходы и эффективность защиты
Overhead and Protection Efficiency

Уровень защиты	Накладные расходы (% CPU)	Точность обнаружения	Время детектирования (мс)
Без защиты	0	–	–
Верификация кода (Code-time)	2–3	100%	–
Контроль контекста (Runtime)	3–5	92%	5
Полная защита + детектирование	8–12	96%	15

Заключение

Предложенная архитектура, интегрированная в полиморфные сетевые модели, обеспечивает комплексный контроль целостности на этапах загрузки, выполнения и обнаружения аномалий. Экспериментально подтверждены приемлемые накладные расходы (8–12 %) и высокая эффективность обнаружения аномалий (96 %), что допустимо для систем мягкого реального времени.

Список использованных источников

1. Dong J., Li S., Wang Y., Zhang L., Chen W., Liu X. (2022) Multi-Agent Adversarial Attacks for Multi-Channel Communications. Proceedings of AAMAS, 3, 1580–1582.
2. Ревотюк М. П., Хаджинова Н. В. (2006) Полиморфные сетевые модели дискретных процессов. В кн.: Идентификация систем и задачи управления (SICPRO'06): материалы Пятой международной конференции. Москва, Институт проблем управления им. В.А. Трапезникова РАН, с. 2042–2158.

References

1. Dong J., Li S., Wang Y., Zhang L., Chen W., Liu X. (2022) Multi-Agent Adversarial Attacks for Multi-Channel Communications. Proceedings of AAMAS, 3, 1580–1582.
2. Revotyuk M. P., Khajynava N. V. (2006) Polymorphic Network Models of Discrete Processes. In: Identification of Systems and Control Problems (SICPRO'06): Proceedings of the Fifth International Conference. Moscow, Institute of Control Sciences, pp. 2042–2158 (in Russian).

Сведения об авторах

Хаджинова Н.В., старший преподаватель кафедры ИТАС, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», khajynova@bsuir.by.

Information about the authors

Khajynava N.V., Senior Lecturer at the Department of Information Technologies of Automated Systems, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, khajynova@bsuir.by.

УДК 538.945

КРИТЕРИИ СМЯГЧЕНИЯ ФОНОННОГО СПЕКТРА МОНОАТОМНОЙ КРИСТАЛЛИЧЕСКОЙ ПЛЕНКИ С ДВУМЕРНЫМ ПОКРЫТИЕМ

В.Н. Кушнир¹, С.Л. Прищепа²

¹Белорусский государственный университет,
г. Минск, Республика Беларусь

² Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной работе анализируется метод априорной оценки параметров двумерной кристаллической структуры, покрывающей тонкую металлическую пленку, необходимых для стабилизации (стимуляции) ее сверхпроводящего состояния. Метод основан на вычислении следа невозмущенной и возмущенной динамической матрицы. В работе рассмотрены два примера одномерных моделей, для которых задача о параметрах возмущения, необходимых для смягчения фононного спектра, решается в явных формулах.

Ключевые слова: Сверхпроводимость; критическая температура; ниобий; графен; модель Борна – Кармана; динамическая матрица; след матрицы; собственные частоты; одномерная цепочка; приближение ближайших соседей.

CRITERIA FOR SOFTENING THE PHONON SPECTRUM OF A MONOATOMIC CRYSTALLINE FILM WITH 2D COATING

V.N. Kushnir¹, S.L. Prischepa²

¹*Belarusian State University, Minsk, Republic of Belarus*

²*Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus*

Abstract. This paper analyzes a method for a priori estimating the parameters of a two-dimensional crystal structure covering a thin metal film, which are necessary for stabilizing (stimulating) its superconducting state. The method is based on calculating the trace of the unperturbed and perturbed dynamic matrices. Two examples of one-dimensional models are considered, for which the problem of determining the perturbation parameters necessary for softening the phonon spectrum is solved using explicit formulas.

Keywords: Superconductivity, critical temperature; niobium; graphene; Born – von Karman model; dynamical matrix; trace of matrix; eigen frequencies; one-dimensional chain; nearest-neighbors approximation.

Введение

Устойчивость характеристик сверхпроводимости пленок наноразмерных толщин относительно вариаций их материальных параметров является необходимым условием использования таких пленок в сверхпроводниковой наноэлектронике и спинтронике. С этой позиции ценность представляет обнаруженный эффект стабилизации критической температуры пленки ниобия при ее покрытии графеном [1]. Трактровка эффекта дана в [1] в рамках концепции стимуляции сверхпроводимости за счет «смягчения» фононного спектра кристаллической решетки (то есть, увеличения статистического веса низких частот). Данная концепция сформировалась к середине 1970-х гг. в ряде основополагающих экспериментальных и теоретических работ – их анализ был выполнен в обзоре [2]. Между тем, достижение эффекта смягчения фононного спектра модификацией поверхности пленки каким-либо 2D-покрытием оказывается довольно случайным событием [2]. Следовательно, необходимы априорные (и простые) критерии эффекта, например, минимума суммы частот, или квадратов частот спектра. Вторым критерий представляется более предпочтительным, поскольку сводится к оценке разности следов невозмущенной и возмущенной динамической матрицы кристаллической решетки. Ниже мы показываем на простых примерах эффективность данного критерия (см. также [3]).

Основная часть

Пусть D_0 и D – динамические матрицы невозмущенной и возмущенной (двумерным покрытием) моноатомной кристаллической

пленки, соответственно. Критерием смягчения фононного спектра назовем соотношение

$$Cr = Tr(D_0) - Tr(D) > 0, \quad (1)$$

где символ Tr означает «след».

В общем случае величина Cr может быть рассчитана в соответствии с теорией И.М. Лифшица [3], однако здесь мы рассмотрим два простых примера, демонстрирующих эффективность критерия, и требующих почти только устного вычисления.

В первом примере рассматривается классическая одномерная гармоническая цепочка N частиц массы M_0 с упругим взаимодействием (жесткости K_0) между ближайшими соседями, дополненная звеном из двух атомов массы M ; принимается, что связь между дополнительными атомами (K), равно как и между основной цепочкой и дополнительной (K_{01}) – также упругая. Данная элементарная модель использовалась в [1] в качестве иллюстрации эффекта смягчения фононного спектра за счет графенового покрытия. Теперь, вводя для этой модели параметры $K_0/M_0 = \omega_0^2$, $K/M = \omega^2$, $K_{01}/K_0 = \alpha$, и используя (1), получим

$$Cr = 4\omega_0^2 - 2\omega^2 - \alpha(1 + M_0/M) > 0. \quad (2)$$

Видим, что условие смягчения фононного спектра, совершенно предсказуемо: собственная частота дополнительного звена, $2^{1/2}\omega$, меньше верхней грани, $2\omega_0$, частотного спектра основной цепочки, связь с ней дополнительного звена должна быть достаточно слабой. Вместе с тем (2), определяя довольно узкую область значений параметров, объясняет безуспешные попытки стимулирования сверхпроводимости разными способами модификации поверхности пленки.

Рассмотрение второго примера связано с тем, что для воспроизведения реальных фононных спектров на основе модели Борна – Кармана учитывалось, как это следует из литературы [4] (см. также [2]), взаимодействие атома с несколькими ближайшими соседями (например, для ниобия необходимое их число равно 10–12). Поэтому, соблюдая последовательность в постановке задач, рассмотрим снова одномерную цепочку с дополнительным 2-атомным звеном, но вначале – с учетом всех парных взаимодействий. В этом случае вместо формулы (2) имеем

$$Cr / \omega_0^2 = 4 \sum_{n=1}^{N-3} \beta_n + 2 \sum_{n=N-2}^{N-1} \beta_n - 2v^2 - \frac{M + M_0}{M} \sum_{i=1}^2 \sum_{n=1}^{N-2} \alpha_{i,n} > 0, \quad (3)$$

где все «жесткости» масштабируются на K_0 (тогда $\beta_1 = 1$) и преобразуются в параметры связи β_n (для основной цепочки) и $\alpha_{i,n}$ (цепочки и звена), а $v = \omega/\omega_0$.

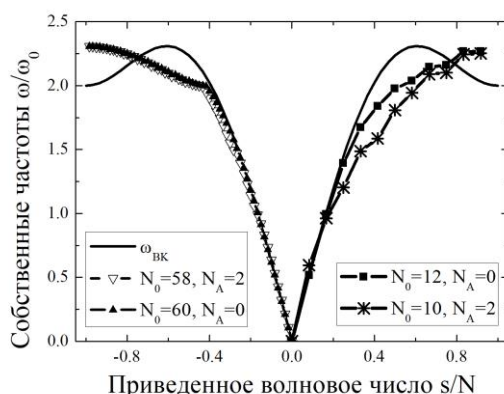
Видим, что принципиально выводы относительно смягчения фонового спектра не меняются, однако существуют обстоятельства, на которых акцентируем внимание, рассмотрев для удобства модель только двух ближайших соседей. В этом случае соотношение (3) упростится:

$$Cr/\omega_0^2 = 4(1+\beta) - 2v^2 - (1 + M_0/M)(\alpha_1 + 2\alpha_2) > 0. \quad (4)$$

Зафиксировав отношение M_0/M и β , получим из (4) область значений в пространстве трех параметров (v , α_i), благоприятных для сверхпроводимости. Факт смягчения фонового спектра при условии положительного критерия мы иллюстрируем на рисунке сравнением спектров однородной цепочки с числом одинаковых «атомов» $N_0 = 12$ (число дополнительных атомов $N_A = 0$) и цепочки с дополнительным звеном двух легких атомов ($N_0 = 10$, $N_A = 2$). Для расчета зафиксировано отношение $M_0/M = 7.5$ (близкое к отношению масс атомов Nb и C) и $\beta = 0.75$, взяты значения $v^2 = 0.5$, $\alpha_1 = 0.1$, а параметр α_2 находится из принятого значения $Cr = 4$. Из рисунка мы видим, что на участке $(0.2, 0.8)$ приведенных волновых чисел возмущенный спектр (звездочки) лежит ниже невозмущенного (квадратные символы).

Следующий факт, на который следует обратить внимание, заключается в характере дисперсионных кривых возмущенной и невозмущенной цепочки при $N_0 \rightarrow \infty$; из рисунка видим, что они почти сливаются (для удобства они представлены с отрицательными приведенными волновыми числами).

Наконец, обратим внимание на интересный сопутствующий факт, отраженный на рисунке: спектр «разомкнутой» цепочки в области высоких частот не совпадает со спектром цепочки, замкнутой по циклическим условиям Борна – Кармана. Этот факт обязан включению дополнительной связи со значением параметра $\beta > 0.25$.



Дисперсионные кривые невозмущенной и возмущенной упругой цепочки (линии с символами) и дисперсионная кривая одномерной периодической цепочки
Dispersion curves of unperturbed and perturbed elastic chains (lines with symbols) and the dispersion curve of a one-dimensional periodic chain

Заключение

Таким образом, простота и эффективность рассмотренного критерия смягчения фононного спектра в одномерных задачах убеждают в перспективности его обобщения на случай реальных монокристаллических решеток.

Список использованных источников

1. Prischepa S. L., Kushnir V. N., Cirillo C., Granata V., Komissarov I. V., Kovalchuk N. G., et al. (2021) Superconducting critical temperature and softening of the phonon spectrum in ultrathin Nb and NbN/graphene hybrids. *Superconductor Science and Technology. IOP*. 34, 115021-1–15.
2. Prischepa S. L., Kushnir V. N. (2023) Phonon softening in nanostructured phonon-mediated superconductors (review). *Journal of Physics: Condensed Matter. IOP*. 35, 313003-1–54.
3. Лифшиц И. М. (1952) Об одной задаче теории возмущений, связанной с квантовой статистикой. *Успехи математических наук*. 7(1) 171–180.
4. Nakagawa Y., Woods A. D. B. (1963) Lattice dynamics of niobium. *Physical Review Letters. APS*. 11(6) 271–274.

References

1. Prischepa S. L., Kushnir V. N., Cirillo C., Granata V., Komissarov I. V., Kovalchuk N. G., et al. (2021) Superconducting critical temperature and softening of the phonon spectrum in ultrathin Nb and NbN/graphene hybrids. *Superconductor Science and Technology. IOP*. 34, 115021-1–15.
2. Prischepa S. L., Kushnir V. N. (2023) Phonon softening in nanostructured phonon-mediated superconductors (review). *Journal of Physics: Condensed Matter. IOP*. 35, 313003-1–54.
3. Lifshitz I. M. (1952) On a problem of the theory of perturbations connected with quantum statistics. *Uspekhi Matematicheskikh Nauk*. 7(1) 171–180 (in Russian).
4. Nakagawa Y., Woods A. D. B. (1963) Lattice dynamics of niobium. *Physical Review Letters. APS*. 11(6) 271–274.

Сведения об авторах

Кушнир В.Н., д-р физ.-мат. наук, доц., проф., Белорусский государственный университет, vnkushnir@gmail.com.

Прищепа С.Л., д-р физ.-мат. наук, проф., проф., учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», prischepa@bsuir.by.

Information about the authors

Kushnir V.N., Dr. Sci. (Phys. Mat.), Associate Professor, Professor of the Department, Belarusian State University, vnkushnir@gmail.com.

Prischepa S.L., Dr. Sci. (Phys. Mat.), Professor, Professor, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, prischepa@bsuir.by.

УДК 004.056:621.397

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЦИФРОВОЙ СИСТЕМЫ IP-ВИДЕОНАБЛЮДЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТА НАБЛЮДЕНИЯ

М.А. Боровой, Ч.В. Ободо

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматриваются возможности цифровых систем IP-видеонаблюдения в обеспечении безопасности объектов. Проведен анализ функциональных требований к современным системам видеоконтроля, включая качество видеозаписи, хранение архивов, удаленный доступ и интеграцию с другими средствами охраны. Особое внимание уделяется преимуществам IP-технологий, таким как масштабируемость, надежность и многопользовательский режим. Показано, что внедрение IP-видеонаблюдения позволяет существенно повысить эффективность контроля и уровень защищенности объектов.

Ключевые слова: IP-видеонаблюдение; системы безопасности; видеоконтроль; удаленный доступ; видеозапись; хранение данных; Wi-Fi-камеры; интеграция систем; охрана объектов; цифровые технологии.

ANALYSIS OF THE CAPABILITIES OF A DIGITAL IP VIDEO SURVEILLANCE SYSTEM TO ENSURE THE SECURITY OF THE OBJECT UNDER SURVEY

M.A. Borovoy, Ch.W. Obodo

*Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus*

Abstract. This article examines the potential of digital IP video surveillance systems for ensuring facility security. It analyzes the functional requirements for modern video surveillance systems, including video recording quality, archival storage, remote access, and integration with other security tools. Particular attention is paid to the advantages of IP technologies, such as scalability, reliability, and multi-user capabilities. It is demonstrated that the implementation of IP video surveillance significantly improves monitoring efficiency and facility security.

Keywords: IP video surveillance; security systems; video control; remote access; video recording; data storage; Wi-Fi cameras; systems integration; facility security; digital technologies.

Введение

В настоящее время системы видеонаблюдения стали неотъемлемым элементом повседневной жизни. Рынок предлагает широкий спектр подобных систем, оснащенных разнообразными функциями: запись по детекции движения или звука, настройка по расписанию, регулировка чувствительности встроенных датчиков, выделение значимых кадров. Такие возможности позволяют осуществлять эффективный контроль

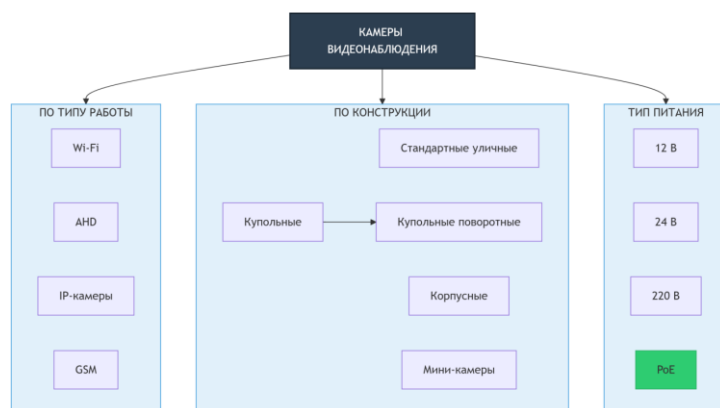
над охраняемой территорией и обеспечивать необходимый уровень защиты жилых объектов, офисных помещений и материальных ценностей

Основная часть

Проведенный анализ позволяет выделить ключевые требования, предъявляемые к современным системам видеонаблюдения. В их число входят высокое качество записи видеоизображения, возможность съемки в условиях недостаточной освещенности, а также запись звука с видеокамер. Существенное значение имеет глубина хранения видеоархива, которая должна составлять не менее 30 суток, и возможность оперативного доступа к архивным материалам. Важными требованиями выступают удаленный просмотр в режиме реального времени через мобильные устройства, дистанционный доступ к видеоархиву, а также возможность модернизации системы и наращивания количества камер. Дополнительную гибкость обеспечивает поддержка беспроводных Wi-Fi-камер, функция подачи сигнала тревоги, надежность оборудования, минимизация «мертвых» зон при максимизации угла обзора и организация резервного электропитания.

Реализация перечисленных функций позволяет IP-видеонаблюдению выступать в роли ключевого элемента при построении комплексной системы охраны объекта. Среди основных преимуществ IP-систем следует отметить возможность интеграции с иными охранными комплексами, дистанционный контроль объекта, многопользовательский режим работы, расширенный функционал, а также высокую надежность и управляемость.

Использование интернет-ресурсов в IP-системах видеонаблюдения обеспечивает возможность мониторинга объекта из любой точки за его пределами. Для этого достаточно наличия мобильного устройства и доступа к глобальной сети. Кроме того, контроль объекта, а также запись, воспроизведение, сортировка и архивирование видеоданных могут осуществляться одновременно несколькими операторами.



Классификация камер видеонаблюдения по различным параметрам
Classification of CCTV cameras by various parameters

Заключение

Таким образом, IP-система видеонаблюдения характеризуется высоким качеством передачи видео- и аудиосигнала, поддержкой Wi-Fi-камер, а также возможностью последующего расширения и модернизации охранного комплекса. Указанные особенности позволяют рассматривать ее в качестве базового элемента организации видеонаблюдения как эффективного инструмента повышения уровня безопасности объекта.

Список использованных источников

1. Акперов И.Г., Сметанин А.В., Коноплева И.А. (2014) *Информационные технологии в менеджменте: учебник*. Москва, Издательский дом «Инфра-М».
2. Будзинский Н. В., Дамьяновски В., Зайцев А. Г. и др. (2015) *Системы охранного телевидения*. Москва, ООО «Ай-Эс-Эс Пресс».
3. Лыткин А. (2016) *IP-видеонаблюдение: наглядное пособие*. Москва, Издательство «Секьюрити Фокус».

References

1. Akperov I. G., Smetanin A. V., Konopleva I. A. (2014) *Information technologies in management: textbook*. Moscow, Infra-M Publishing house (in Russian).
2. Budzinsky N. V., Damyanovsky V., Zaitsev A. G. et al. (2015) *Security television systems*. Moscow, ISS Press LLC (in Russian).
3. Lytkin A. (2016) *IP video surveillance: a visual aid*. Moscow, Security Focus Publishing House (in Russian).

Сведения об авторах

Боровой М.А., ст. гр. 561401 факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», maksimborovoj1@gmail.com.

Ободо Ч.В., магистрант гр. 567311 каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», chidozieobodo13@gmail.com.

Information about the authors

Borovoy M.A., student of group 561401, Faculty of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, maksimborovoj1@gmail.com.

Obodo Ch.W., Postgraduate Student gr. 567311, Department of Information Security, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, chidozieobodo13@gmail.com.

УДК 621.3.049.772

АЛЮМООКСИДНЫЕ КОРПУСА ДЛЯ ЗАЩИТЫ МИКРОСХЕМ ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ

С.К. Лазарук¹, Т.И. Ореховская¹, В.В. Дудич¹, А.В. Долбик¹,
Л.П. Томашевич¹, С.А. Ефименко²

¹ Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь

²ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ»,
Минск, Республика Беларусь

Аннотация. Разработана конструкция алюмооксидного корпуса интегральных микросхем, обладающего повышенными защитными свойствами при воздействии внешних электромагнитных полей. Экранирование внешних электромагнитных воздействий осуществляется за счет алюминиевого каркаса основания корпуса. Обсуждены способы защиты микросхем в алюмооксидном корпусе от γ -излучения за счет использования вольфрамовой крышки корпуса, что важно для эксплуатации микросхем в космических устройствах.

Ключевые слова: алюминий; электрохимическое анодирование; анодный оксид алюминия; алюмооксидный корпус, микросхема, экранирование.

ALUMINA PACKAGES FOR PROTECTING MICROCIRCUITS FROM EXTERNAL INFLUENCES

S.K. Lazarouk¹, T.I. Orekhovskaya¹, V.V. Dudich¹, A.V. Dolbik¹,
L.P. Tomashevich¹, S.A. Efimenko²

¹Educational Institution "Belarusian State University of Informatics and
Radioelectronics", Minsk, Republic of Belarus

²JSC "INTEGRAL" – "INTEGRAL" Holding Managing Company.s

Abstract. A design for an alumina housing for integrated circuits has been developed. It offers enhanced protective properties against external electromagnetic fields. Shielding from external electromagnetic influences is achieved through the use of an aluminum frame at the housing base. Methods for protecting alumina-housed microcircuits from γ -radiation by using a tungsten housing cap are discussed, which is important for the use of microcircuits in space devices.

Keywords: aluminum; electrochemical anodizing; anodic aluminum oxide; alumina package, microcircuit, shielding.

Корпус интегральной микросхемы обеспечивает защиту кристалла микросхемы от внешних воздействий и электрические соединения с внешними электронными устройствами. В алюмооксидных корпусах, формируемых локальным анодированием алюминия, электрические соединения с кристаллом осуществляются через сквозные алюминиевые электроды, встроенные в алюмооксидное основание корпуса [1–9]. В данной работе разработана конструкция алюмооксидных корпусов интегральных микросхем с целью их защиты от внешнего

электромагнитного поля и других воздействий, влияющих на работоспособность электронных устройств.

Алюмооксидный корпус состоит из контактной монтажной площадки (основание корпуса) и металлической крышки. Контактная монтажная площадка состоит из сквозных алюминиевых электродов, встроенных в анодный оксид алюминия, и алюминиевой рамки, определяющей внешние границы корпуса. Алюминиевые электроды обеспечивают соединение микросхемы с внешними электронными устройствами, а оксид алюминия, сформированный локальным анодированием алюминиевых пластин с использованием фотолитографической маски, обеспечивает изоляцию алюминиевых электродов.

Измерения электрофизических параметров алюмооксидных корпусов показали следующие результаты. Токи утечки при напряжениях до 300 В не превышали 1 пА, что свидетельствует о преимуществах данной конструкции по сравнению с аналогами (пластмассовые и керамические корпуса). Тепловое сопротивление данной конструкции составляет менее 1°С/Вт. Низкое значение теплового сопротивления обеспечивается за счет высокой теплопроводности алюминия, что позволяет эффективно рассеивать тепло в процессе работы микросхем и свидетельствует о преимуществе разработанной контактной площадки. Исследование механической прочности позволило оценить давление (20-40 МПа), приводящее к разрушению основания корпуса. Полученный диапазон давления свидетельствует о достаточной механической прочности сформированного изделия. Следует отметить, что алюминий обладает высокой эластичностью, что позволяет смягчать механические напряжения, возникающие между кремниевыми кристаллами и основанием корпуса при термическом разогреве в процессе их функционирования [10].

Важной особенностью разработанной конструкции является защита микросхем от внешнего электромагнитного излучения, что достигается за счет эффективного экранирования данного излучения металлическим каркасом основания корпуса, составляющем большую его объемную часть. Также разработанная конструкция обеспечивает защиту от α -, β -излучения, а в случае изготовления крышки корпуса из вольфрама может быть реализована защита от γ -излучения, что важно для использования электронных устройств в космических спутниках.

Таким образом, разработанная конструкция алюмооксидных корпусов способна обеспечить защиту от внешнего электромагнитного излучения, что может быть использовано при корпусировании специализированных микросхем, функционирующих в условиях сильных электромагнитных полей и радиационных воздействий.

Список использованных источников / References

1. Lazarouk S. K., Bondarenko V. P., Borisenko V. E., Gaponenko N. V., Gorokh G. G., Leshok A.A., . al. (2024) Perspective Optical and Electronic Interconnects of Integrated Circuit Elements. *Doklady BGUIR*. 22 (2), 7-19.
2. Monica S. La, Maiello G., Ferrari A., Masini G., Lazarouk S., Jaguiro P., et. al. (1997) Progress in the field of integrated optoelectronics based on porous silicon. *Thin Solid Films*. 297 (1-2), 265-267.
3. Lazarouk S.K., Leshok A.A., Kozlova T.A., Dolbik A.V., Vi L.D., Ilkov V.K., et. al. (2019) 3D Silicon Photonic Structures Based on Avalanche LED with Interconnections Through Optical Interposer. *International Journal of Nanoscience*. 18 (3-4), 1940091.
4. Lazarouk S., Bondarenko V., Pershukevich P., Monica S. La, Maiello G. (1994) Visible Electroluminescence from Al-Porous Silicon Reverse Bias Diodes Formed on the Base of Degenerate n-Type Silicon. *MRS Online Proceedings Library Archive*. 358, 659–664.
5. Lazarouk S. K., Sasinovich D. A., Katsuba, P. S., Labunov V. A., Leshok A. A., Borisenko V. E. (2007) Electroluminescence from nanostructured silicon embedded in anodic alumina. *Semiconductors*. 41 (9), 1109-1112.
- 6 Bertolotti M., Carassiti F., Fazio E., Ferrari A., Monica S. La, Lazarouk S., et. al. (1995) Porous silicon obtained by anodization in the transition regime. *Thin Solid Films*. 255 (1-2), 152-154.
- 7 Lazarouk S., Jaguiro P., Katsouba S., Monica S. La, Maiello G., Masini G., et. al. (1996) Visible light from aluminum-porous silicon Schottky junctions. *Thin Solid Films*. 276 (1-2), 168-170.
8. Lazarouk S., Muravski A., Sasinovich D., Chigrinov V., Kwok H. S. (2007) Porous and pillar structures formed by. anodization for vertical alignment of nematic liquid crystal. *Japanese Journal of Applied Physics*. 46 (10R), 6889.
9. Lazarouk S.K., Dolbik A.V., Labunov V.A., Borisenko V.E. (2013) Physics, Chemistry and Application of Nanostructures. *World Sci., Singapore*. 355-358.
10. Chelyadinsky A. R., Dorofeev A. M., Kazuchits N. M., Monica S. La, Lazarouk S. K., Maiello G., et. al. (1997) Deformation of porous silicon lattice caused by absorption/desorption processes. *Journal of the Electrochemical Society*. 144 (4), 1463-1468.

Сведения об авторах

Лазарук С.К., доктор физико-математических наук, профессор, заведующий НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», serg@nano.bsuir.edu.by.

Ореховская Т.И., ведущий инженер-технолог НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Дудич В.В., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Долбик А.В., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Томашевич Л.П., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Ефименко С.А., кандидат технических наук, главный конструктор, заведующий лабораторией ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ».

Information about the authors

Lazarouk S., Dr. of Sci. (Phys. and Math.), Professor, Head of the R&D Lab. 4.6 “Integrated Micro- and Nanosystems”, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, serg@nano.bsuir.edu.by.

Orekhovskaya T., Leading Technologist of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Dudich V., Researcher of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Dolbik A., Researcher of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Tomashevich L., Researcher of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Efimenko S.A., Candidate of Technical Sciences, Chief Designer, Head of Laboratory, JSC INTEGRAL – the management company of the INTEGRAL holding company.

УДК 538.975

РЕГУЛЯРНЫЕ МЕТАЛЛИЧЕСКИЕ МАТРИЦЫ ДЛЯ УПРАВЛЕНИЯ ОТРАЖЕНИЕМ ЭЛЕКТРОМАГНИТНЫХ ВОЛН ЗА СЧЕТ ЭФФЕКТА ПОВЕРХНОСТНОГО ПЛАЗМОННОГО РЕЗОНАНСА

В.В. Дудич, О.В. Купреева, Т.И. Ореховская, А.В. Долбик

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Разработана методика формирования регулярных алюминиевых сеточных структур на стеклянных подложках. Выбор геометрических размеров упорядоченной металлической сетчатой структуры позволяет управлять ее спектром отражения. Исследованы спектры отражения сформированных структур и разработан метод уменьшения отраженного сигнала на заданной длине волны за счет использования эффекта плазмонного резонанса. и Применение регулярных металлических структур, демонстрирующих эффект плазмонного резонанса, является перспективным направлением для сферы защиты информации.

Ключевые слова: алюминий; электрохимическое анодирование; анодный оксид алюминия; локальное анодирование; плазмонный резонанс; электромагнитное излучение.

REGULAR METAL MATRICES FOR CONTROLLING ELECTROMAGNETIC WAVES REFLECTION DUE TO THE EFFECT OF SURFACE PLASMON RESONANCE

V.V. Dudich, O.V. Kupreeva, T.I. Orekhovskaya, A.V. Dolbik

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. A method for forming regular aluminum mesh structures on glass substrates has been developed. Selecting the geometric dimensions of the ordered metal mesh structure allows for control of its reflectance spectrum. The reflectance spectra of the resulting

structures have been studied, and a method for reducing the reflected signal at a given wavelength has been developed using the plasmon resonance effect. The use of regular metal structures exhibiting plasmon resonance is a promising area for information security.

Keywords: aluminum; electrochemical anodizing; anodic aluminum oxide; local anodization; plasmon resonance; electromagnetic radiation.

Поверхностный плазмонный резонанс – это физическое явление, при котором электромагнитные волны возбуждают коллективные колебания свободных электронов (плазмонов) по границе металла и диэлектрика [1, 2]. Это вызывает резонансное поглощение света на длине волны определяемой геометрическими размерами упорядоченной металлической структуры на диэлектрической поверхности. В данной работе были изготовлены регулярные алюминиевые сеточные структуры на стеклянных подложках и исследованы их спектры отражения.

Исследуемые плазмонные структуры формировали магнетронным осаждением алюминиевых пленок, толщиной 1 мкм, на стеклянные подложки с последующим локальным анодированием алюминия [3] с использованием фоторезистивной маски для формирования сетчатых структур с периодом 20 мкм при ширине алюминиевой дорожки порядка 2 мкм. Спектры отражения измерялись как в видимом, так и в инфракрасном диапазоне.

Сформированные сетчатые структуры пропускали 80-90 % светового сигнала в видимом и ближнем ИК-диапазонах [4], что подтверждает прозрачность анодного оксида алюминия в данных оптических диапазонах. В диапазоне 18-22 мкм (средний ИК диапазон) наблюдается явление плазмонного резонанса – поглощение на длине волны 19,5 мкм, а на краях вышеотмеченного диапазона наблюдалось отражение более 20 %. [5–9]

Таким образом показано, что выбор геометрических размеров упорядоченной металлической сетчатой структуры позволяет управлять ее спектром отражения, что представляет интерес для маскирования объектов при их обнаружении локацией на заданной длине волны.

Проведенные исследования позволили разработать метод уменьшения отраженного сигнала на заданной длине волны за счет использования эффекта плазмонного резонанса в упорядоченных металлических сетчатых структурах на диэлектрических подложках, что является одним из технических средств защиты охраняемой информации.

Работа выполнена при финансовой поддержке БРФФИ НАН РБ (договор T26B-010).

Список использованных источников / References

1. Nguyen H.T., Hoang T.T., Nguyen X.B., Dung T.Q., Pham T.S., Le K.Q. (2022) Enhanced near-infrared fluorescent sensing using metal-dielectric-metal plasmonic array. *Plasmonics* 17 (6), 2337-2344.
2. Dolbik A.V., Sasinovich D.A., Zavadskii S.M., Golosov D.A., Meledina M.V., et. al. (2025) Optical Properties of Transparent Conducting Coatings Based on an Aluminum Grid Embedded in Anodic Aluminum Oxide. *Surface Engineering and Applied Electrochemistry* 61 (3), 333-337.
3. Lazarouk S., Bondarenko V., Pershukovich P., Monica S. La, Maiello G. (1994) Visible Electroluminescence from Al-Porous Silicon Reverse Bias Diodes Formed on the Base of Degenerate n-Type Silicon. *MRS Online Proceedings Library Archive*. 358, 659–664.
4. Monica S. La, Maiello G., Ferrari A., Masini G., Lazarouk S., Jaguiro P., et. al. (1997) Progress in the field of integrated optoelectronics based on porous silicon. *Thin Solid Films*. 297 (1-2), 265-267.
5. Lazarouk S., Jaguiro P., Katsouba S., Monica S. La, Maiello G., Masini G., et. al. (1996) Visible light from aluminum-porous silicon Schottky junctions. *Thin Solid Films*. 276 (1-2), 168-170.
6. Lazarouk S.K., Leshok A.A., Kozlova T.A., Dolbik A.V., Vi L.D., Ilkov V.K., et. al. (2019) 3D Silicon Photonic Structures Based on Avalanche LED with Interconnections Through Optical Interposer. *International Journal of Nanoscience*. 18 (3-4), 1940091.
7. Lazarouk S. K., Sasinovich D. A., Katsuba, P. S., Labunov V. A., Leshok A. A., Borisenko V. E. (2007) Electroluminescence from nanostructured silicon embedded in anodic alumina. *Semiconductors*. 41 (9), 1109-1112.
8. Lazarouk S., Jaguiro P., Katsouba S., Masini G. (1996) Stable electroluminescence from reverse biased n-type porous silicon–aluminum Schottky junction device. *Appl. Phys. Lett* 68 (15), 2108.
9. Jaguiro P., Katsuba P., Lazarouk S., Moore S., Smirnov A. (2009) *Physica E: Low-Dimensional Systems and Nanostructures* 41 (6), 1094-1096.

Сведения об авторах

Дудич В.В., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». dudich@bsuir.by

Купреева О.В., кандидат физико-математических наук, старший научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kupreeva@bsuir.by.

Ореховская Т.И., ведущий инженер-технолог НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Долбик А.В., научный сотрудник НИЛ 4.6, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Dudich. V., Researcher of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”. dudich@bsuir.by

Kupreeva O., Ph.D. (Phys. and Math.), Senior Researcher of the R&D Lab. 4.6 “Integrated Micro- and Nanosystems”, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, kupreeva@bsuir.by.

Orekhovskaya T., Leading Technologist of the R&D Lab. 4.6, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Dolbik A., Researcher of the R&D Lab. 4.6 Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

УДК 377.3

ОСОБЕННОСТИ ПРАКТИКО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СРЕДНИМ СПЕЦИАЛЬНЫМ ОБРАЗОВАНИЕМ

В.В. Шаталова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь

Аннотация. В статье рассмотрены основные особенности практико-ориентированной подготовки специалистов среднего звена в области информационной безопасности с учетом реализации требований образовательного стандарта и подготовки высококвалифицированных специалистов учитывая современные требования рынка труда, уровня организации и обеспечения функционирования систем информационной безопасности.

Ключевые слова: информационная безопасность; специалист по информационно безопасности; образовательный стандарт; техническое обеспечение информационной безопасности; практико-ориентированная подготовка специалистов.

FEATURES OF PRACTICE-ORIENTED TRAINING OF INFORMATION SECURITY SPECIALISTS WITH SECONDARY SPECIALIZED EDUCATION

V.V. Shatalova

*Educational institution “Belarusian State University of Informatics and Radioelectronics” branch “Minsk Radio Engineering College”,
Minsk, Republic of Belarus*

Abstract. The article considers the main features of practice-oriented training of middle-level specialists in the field of information security, taking into account the implementation of the requirements of the educational standard and the training of highly qualified specialists, taking into account the modern requirements of the labor market, the level of organization and ensuring the functioning of information security systems.

Keywords: information security; information security specialist; educational standard; technical support of information security; practice-oriented training of specialists.

Введение

В соответствии с ОКРБ 011-2022 «Специальности и квалификации» специальность 5-04-0611-02 «Техническое обеспечение информационной безопасности» относится к профилю образования «Информационные

и коммуникационные технологии», группе специальностей «Прикладные информационные и коммуникационные технологии», что позволяет сформировать определенные профессиональные компетенции, включающие знания и умения по осуществлению мониторинга и регистрации сведений, необходимых для защиты объектов информационной инфраструктуры, сети электросвязи, в том числе с использованием программных и программно-аппаратных средств обнаружения; контролю за эффективным использованием технических средств защиты информации; проведению стандартных и сертификационных испытаний; осуществление диагностики, устранение отказов, обеспечение работоспособности и тестирование функций программных и программно-аппаратных средств обеспечения информационной безопасности; выбору оптимальных решений при планировании работ в условиях нестандартных ситуаций; осуществление выбора программных средства и криптографических методов защиты компьютерной информации и др. [1].

Основная часть

Реализация процесса обучения подготовки кадров в отрасли информационной безопасности в колледже носит практико-ориентированный характер. Обучение строится на проектном методе, который позволяет развивать творческие и познавательные процессы, критическое мышление, умение самостоятельно получать знания и применять их в практической деятельности, ориентироваться в информационном пространстве.

Такой подход позволяет систематизировать полученные знания и умения на учебных предметах, реализовать практическое исполнение курсовых проектов, а также решать различные исследовательские задачи, поставленные преподавателями учреждения образования и системно подготовиться к выполнению дипломного проекта с возможной практической реализацией, направленной на решение конкретной производственной задачи с привлечением специалистов с предприятий заказчиков - кадров, решение которых требует от учащихся использования интегрированных знаний в различных областях. Кроме того, активно применяются электронные учебники и онлайн-ресурсы. Формирование профессиональных компетенций реализуется через изучение трех основных модулей: модуль «Информационная безопасность и программирование», модуль «Программные средства обеспечения информационной безопасности» и модуль «Технические средства обеспечения информационной безопасности». Обучение тесно связано с работой в лаборатории защиты информации, где учащиеся изучают аппаратное обеспечение, занимаются настройкой и монтажом

инженерно-технических средств охраны, работают с аппаратными блокираторами. Именно здесь на практических занятиях, а также в ходе учебных практик учащиеся осваивают методы мониторинга, диагностики и нейтрализации угроз в компьютерных системах.

Лаборатория защиты информации – специализированная учебная площадка, предназначенная для формирования практических компетенций в области выявления и блокирования каналов утечки данных, которая представляет собой высокотехнологичный полигон, оснащенный современными программно-аппаратными комплексами, максимально приближенными к реальной инфраструктуре предприятия.

Здесь создана уникальная среда, позволяющая моделировать различные сценарии нарушения политик безопасности – от внутренних утечек до внешних атак по техническим каналам связи. Оснащение лаборатории позволяет реализовать полный цикл подготовки специалистов, начиная от теоретическо-правовых основ информационной безопасности, криптографические методы защиты информации, защита информации техническими средствами и заканчивая прохождением практического обучения в рамках учебных практик «Информационная безопасность в компьютерных системах» и «Техническая защита информации».



Фотографии лабораторий
Laboratory photoes

Ключевым элементом лаборатории является универсальный испытательный учебно-лабораторный стенд для обучения ЗИ от утечек по акустическим, оптоэлектронному и виброакустическим каналам. Стенд, оснащенный сменными панелями, имитирующими оконные и дверные проемы, а также вентиляционные каналы, позволяет физически оценить реальные каналы утечки и эффективность применяемых средств защиты. Практическая часть обучения в лаборатории подкреплена наличием реального оборудования, используемого в системах физической защиты объектов. Для отработки навыков организации контроля доступа и охраны периметра лаборатория оснащена действующими образцами технических

средств (камера видеонаблюдения, доводчик дверной, система контроля доступа с пропуск-картами, генератор белого шума), что позволяет интегрировать теоретические знания с практическими навыками работы с реальными техническими средствами охраны, контроля доступа и активной технической защиты информации, что является неотъемлемой частью подготовки компетентного специалиста по техническому обеспечению информационной безопасности.

Заключение

Лаборатория также выполняет важную профориентационную функцию, знакомя школьников, абитуриентов и гостей колледжа с перспективной и востребованной специальностью в сфере информационно-коммуникационных технологий. Высокий уровень материально-технической базы в сочетании с квалифицированным преподавательским составом гарантирует подготовку компетентных специалистов, способных решать актуальные задачи обеспечения информационной безопасности на современных предприятиях и в организациях.

Список использованных источников

1. Образовательный стандарт среднего специального образования по специальности 5-04-0611-02 «Техническое обеспечение информационной безопасности»: постановление Министерства образования Республики Беларусь, 30.09.2022, № 347 // Национальный правовой Республики Беларусь [Электронный ресурс]. – 2026. – Режим доступа : <https://pravo.by/>.

References

1. Educational standard of secondary special education in specialty 5-04-0611-02 “Technical support of information security”: Resolution of the Ministry of Education of the Republic of Belarus, 30.09.2022, No. 347 // National Law of the Republic of Belarus [Electronic resource]. – 2026. – Access mode : <https://pravo.by/>.

Сведения об авторах

Шаталова В.В., канд. техн. наук, доц., директор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», shatalova@bsuir.by.

Information about the authors

Shatalova V.V., Cand. Sci., Associate Professor, director, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, branch “Minsk Radio Engineering College”, shatalova@bsuir.by.

УДК 004.056

О XXIV МЕЖДУНАРОДНОЙ ОЛИМПИАДЕ ПО КРИПТОГРАФИИ SARCRIPT

М.Б. Абросимов, А.В. Жаркова, А.А. Лобов, О.В. Моденова, А.А. Саяпина,
З.А. Калашникова, Е.А. Трунилина, А.О. Шабаркова
*ФГБОУ ВО Саратовский научный исследовательский государственный
университет имени Н.Г. Чернышевского, Саратов, Россия*

Аннотация. Статья посвящена подведению итогов XXIV международной олимпиады по криптографии SarCrypt, которая с 2002 года проводится Саратовским научным исследовательским государственным университетом имени Н.Г. Чернышевского. Тематика задач в основном относится к криптографии, стеганографии, теории кодирования, комбинаторике и другим разделам математики и информатики. Для решения задач разрешается использовать любые доступные средства: любые системы программирования, собственные или сторонние программы, справочные материалы, сеть Интернет, большие языковые модели.

Ключевые слова: олимпиада школьников; олимпиада студентов; олимпиада по криптографии; информационная безопасность; криптография.

ABOUT THE XXIV INTERNATIONAL CRYPTOGRAPHY OLYMPIADS SARCRIPT

M.B. Abrosimov, A.V. Zharkova, A.A. Lobov, O.V. Modenova, A.A. Sayapina,
Z.A. Kalashnikova, E.A. Trunilina, A.O. Shabarkova
*Saratov Scientific Research State University named after N.G. Chernyshevsky,
Saratov, Russia*

Abstract. This article summarizes the results of the 24th International Cryptography Olympiad SarCrypt, which has been held by the Saratov State University since 2002. The problems primarily cover cryptography, steganography, coding theory, combinatorics, and other areas of mathematics and computer science. Any available tools may be used to solve the problems: any programming systems, any programs, reference materials, the Internet, and large language models.

Keywords: School Olympiad; Student Olympiad; Cryptography Olympiad; Information Security; Cryptography.

Кафедра теоретических основ компьютерной безопасности и криптографии Саратовского научного исследовательского государственного университета имени Н.Г. Чернышевского провела очередную, 24-ю по счету, открытую олимпиаду по криптографии SarCrypt. Саратовские олимпиады по криптографии проводятся с 2002 года, когда была создана кафедра теоретических основ компьютерной безопасности и криптографии и открыта специальность «Компьютерная безопасность». XXIV олимпиада SarCrypt проводилась в 2025-2026 учебном году. С 2018 года олимпиада проводится в два тура. Традиционно первый тур олимпиады проходит в декабре и является

отборочным. На решение задач первого тура дается одна неделя. На второй тур попадают победители первого тура, то есть участники, занявшие 1–3 место. Проводится второй тур в воскресенье в конце января или в начале февраля. На решение задач очного тура отводится 3 часа. Второй тур традиционно проводится на базе факультета компьютерных наук и информационных технологий Саратовского государственного университета имени Н.Г. Чернышевского. Олимпиада проводится для трех категорий участников: учеников 6–8 классов, 9–11 классов и студентов. Ученикам 6–8 классов обычно предлагается 6 задач, ученикам 9–11 классов – 8 задач, студентам – 10 задач. Тематика задач в основном относится к криптографии, стеганографии, теории кодирования, комбинаторике и другим разделам математики и информатики.

В этом учебном году первый тур проводился 8–15 декабря 2025 года. В отборочном туре приняли участие 370 школьников и студентов: 50 учеников 6–8 классов, 84 ученика 9–11 классов и 236 студентов из городов России, Республики Молдовы и Туркменистана. Все участники I–II туров получили электронные дипломы, а их руководители – грамоты.

Основной особенностью олимпиады является то, что участникам разрешается использовать любые средства для решения задач: Интернет, любые среды для программирования, а также и большие языковые модели, как на отборочном, так и на итоговом туре.

В докладе обсуждаются задачи, которые предлагались участникам, и анализируются итоги олимпиады. Сравняются изменения в подготовке участников по сравнению с предыдущими олимпиадами SarCrypt [1, 2].

Список использованных источников

1. Абросимов М.Б., Салий В.Н., Жаркова А.В., Лобов А.А., Моденова О.В., Конюшенко А.С. и др. (2023) XXI международная олимпиада по криптографии SarCrypt. *Технические средства защиты информации : тез. докл. XXI Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 6 июня 2023 года).* – Минск : БГУИР, 12.

2. Абросимов М.Б., Жаркова А.В., Лобов А.А., Моденова О.В., Саяпина А.А., Улитин И.В. (2024) Анализ результатов XXII международной олимпиады по криптографии SarCrypt. *Технические средства защиты информации : тез. докл. XXII Белорусско-Российской науч.-техн. конф. (Республика Беларусь, Минск, 12 июня 2024 года).* – Минск : БГУИР, 2024, 8-9.

References

1. Abrosimov MB, Saliy VN, Zharkova AV, Lobov AA, Modenova OV, Konyushenko AS, et al. (2023) XXI International Olympiad on Cryptography SarCrypt. *Technical means of information protection: abstract of the report of the XXI Belarusian-*

Russian scientific-technical conf. (Republic of Belarus, Minsk, June 6, 2023). – Minsk: BSUIR, 12 (in Russian).

2 Abrosimov MB, Zharkova AV, Lobov AA, Modenova OV, Sayapina AA, Ulitin IV (2024) Analysis of results of the XXII International Olympiad on Cryptography SarCrypt. Technical means of information protection: abstract of the report. XXII Belarusian-Russian scientific-technical conf. (Republic of Belarus, Minsk, June 12, 2024). – Minsk: BSUIR, 2024, 8-9 (in Russian)

Сведения об авторах

Абросимов М.Б., д-р физ.-мат. наук, проф., зав. каф., ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, mic@rambler.ru.

Жаркова А.В., канд. физ.-мат. наук, доц., доц., ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, zharkovaAV3@gmail.com.

Лобов А.А., зав. лаб., ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, aisaneikai@mail.ru.

Моденова О.В., доц., ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, oginiel@rambler.ru.

Саяпина А.А., студентка, ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, saiapina.aa@mail.ru.

Калашникова З.А., студентка, ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, zlatale@mail.ru.

Трунилина Е.А., студентка, ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, e.trunilina04@mail.ru.

Шабаркова А.О., аспирантка, ФГБОУ ВО Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, shabarkova_alex.andra@mail.ru.

Information about the authors

Abrosimov M.B., Doctor of Physical and Mathematical Sciences, Professor, Head of the Department, Saratov National Research State University named after N.G. Chernyshevsky, mic@rambler.ru .

Zharkova A.V., Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor, Saratov National Research State University named after N.G. Chernyshevsky, zharkovaAV3@gmail.com .

Lobov A.A., Head of the Laboratory, Saratov National Research State University named after N.G. Chernyshevsky, aisaneikai@mail.ru .

Modenova O.V., Associate Professor, Saratov National Research State University named after N.G. Chernyshevsky, oginiel@rambler.ru .

Sayapina A.A., student, Saratov National Research State University named after N.G. Chernyshevsky, saiapina.aa@mail.ru .

Kalashnikova Z.A., student, Saratov National Research State University named after N.G. Chernyshevsky, zlatale@mail.ru .

Trunilina E.A., student, Saratov National Research State University named after N.G. Chernyshevsky, e.trunilina04@mail.ru .

Shabarkova A.O., postgraduate student, Saratov National Research State University named after N.G. Chernyshevsky, shabarkova_alex.andra@mail.ru .

УДК 537.611.2

РАСПРЕДЕЛЕНИЯ НАМАГНИЧЕННОСТИ В НАНОШНУРАХ НИКЕЛЯ

М.В. Шарейко, А.Л. Данилюк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной работе с помощью моделирования в пакете Nmag установлены закономерности изменения распределения намагниченности нанопровов никеля под действием упругих напряжений. Выявленные закономерности перехода намагниченности из перпендикулярного в радиальное состояние определяются размерами нанопровов и его аспектным отношением. Установлено, что с ростом аспектного отношения растет пороговая величина упругих напряжений для такого перехода.

Ключевые слова: нанопровы; никель; намагниченность; магнитоупругие напряжения.

MAGNETIZATION DISTRIBUTIONS IN NICKEL NANOWIRES

M.V. Shareiko, A.L. Danilyuk

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. In this study, using simulations in the Nmag package, the patterns of magnetization distribution changes in nickel nanowires under elastic stress were established. The patterns of magnetization transition from a perpendicular to a radial state depend on the nanowire size and its aspect ratio. As the aspect ratio increases, the threshold elastic stress for this transition increases.

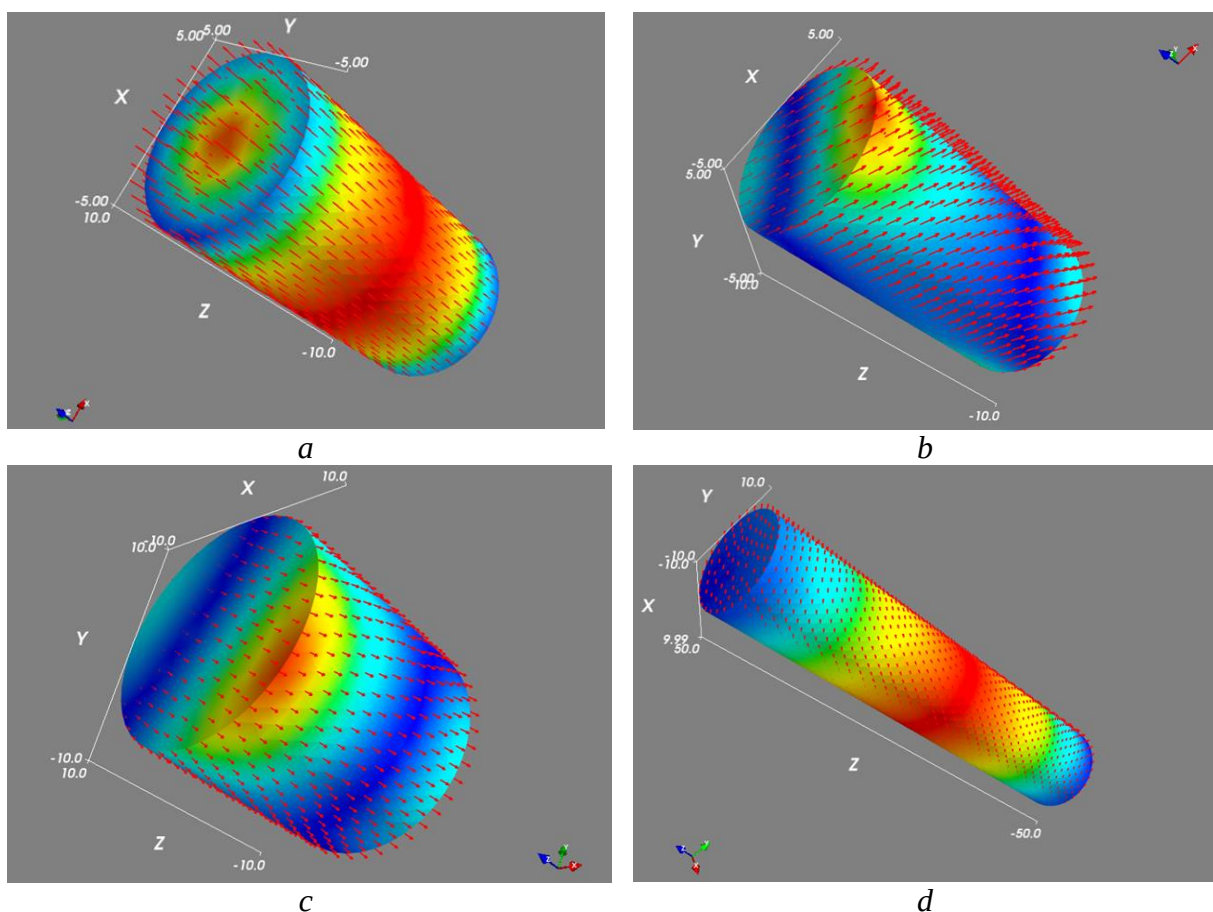
Keywords: nanowires; nickel; magnetization; magnetoelastic stresses.

Введение

Никель (Ni) это ферромагнетик с температурой Кюри 358 °С. При комнатной температуре его намагниченность насыщения составляет 485–490 кА/м (или 0,61–0,64 Тл). Никель обладает кубической кристаллической решеткой. Константа первой анизотропии $(-4,5...-5,0) \cdot 10^3$ Дж/м³) отрицательна. В нанокристаллическом никеле намагниченность насыщения может падать при уменьшении размера (размерный эффект), а растяжение решетки может изменять характер анизотропии.

Основная часть

Для проведения микромагнитного моделирования применялся пакет Nmag, который для расчета намагниченности использует уравнение Ландау-Лифшица-Гильберта [1] и метод конечных элементов [2]. Шаг дискретизации равен от 1 до 2 нм. Проведенное моделирование распределения намагниченности в нанопшнурках никеля показало следующее. Для цилиндра диаметром $D = 10$ нм и высотой $h = 20$ нм в отсутствие напряжений равновесным направлением намагниченности является ось цилиндра (z-состояние), рисунок *a*. При наличии бокового сжатия нанопшнура намагниченность ориентирована перпендикулярно оси цилиндра (т.е. переходит в радиальное состояние), рисунок *b*. Величина перехода составляет $\sigma_{th} = 0,4$ ГПа.



Намагниченность никелевых нанопшнуров разных размеров в отсутствие магнитоупругих напряжений (*a*) и при радиальном сжатии с нагрузкой 0,4 ГПа (*b*), 0,06 ГПа (*c*), 0,6 ГПа (*d*)
Magnetization of nickel nanowires of different sizes in the absence of magnetoelastic stresses (*a*) and under radial compression with a load of 0.4 GPa (*b*), 0.06 GPa (*c*), 0.6 GPa (*d*)

Для цилиндра диаметром $D = 10$ нм и высотой $h = 100$ нм ситуация аналогична. Порог напряжений перехода из z-состояния в радиальное

составляет $\sigma_{th} = 2,9$ ГПа. Для нанOSHнyра диаметром $D = 20$ нм и высотой $h = 20$ нм в отсутствии напряжений намагниченность также однородна и параллельна оси нанOSHнyра. Однако переход из z-состояния в радиальное происходит при достаточно малых напряжениях, т.е. $\sigma_{th} = 0,06$ ГПа (рисунок c). Для нанOSHнyра диаметром $D = 20$ нм и высотой $h = 100$ нм порог напряжений перехода из z-состояния в радиальное составляет $\sigma_{th} = 0,6$ ГПа (рисунок d).

Заклyчение

Таким образом проведенное моделирование для нанOSHнyров никеля показало, что при наличии упругих напряжений магнитная структура может изменяться. В данном случае происходит переход из перпендикулярного z-состояния в радиальное состояние намагниченности при наличии напряжений, сжимающих нанOSHнyр перпендикулярно его оси. Выявленные закономерности перехода намагниченности из перпендикулярного в радиальное состояние определяются размерами нанOSHнyра и его аспектным отношением $a = h/D$. Установлено, что с ростом аспектного отношения растет пороговая величина перехода σ_{th} нанOSHнyра никеля из перпендикулярного в радиальное магнитное состояние.

Полученные закономерности роста пороговой величины напряжений с ростом аспектного отношения определяются прежде всего влиянием анизотропии формы (полями размагничивания), которая противодействует переходу нанOSHнyра в радиальное состояние, так как магнитокристаллическая анизотропия оказывает незначительное влияние. Чем выше вклад анизотропии формы, тем больше должна быть величина магнитоупругой энергии, чтобы достичь перехода. Так как с ростом аспектного отношения вклад анизотропии формы растет, то наблюдается также и увеличение пороговой величины упругих напряжений для перехода из перпендикулярного в радиальное магнитное состояние. Однако рост вклада анизотропии формы с увеличением аспектного отношения не является линейным, он достигает насыщения при аспектном отношении, когда разность размагничивающих факторов для нанOSHнyра перестает практически изменяться. Поэтому для пороговой величины упругих напряжений также должен наблюдаться выход на насыщение.

Список использованных источников

1. Гладков С.О., Богданова С.Б. (2015) К теории уравнения Ландау-Лифшица-Гильберта. *Физика твердого тела*. 57(5), 913–916.
2. J. Vishal, A. Sethi, D-K. Kumar. (2013) Finite Element Method: An Overview. *Walailak Journal of Science and Technology*. 10(1), 1–8.

3 T. Wasiak, L. Przypis, K. Walczak, D. Janas. (2018) Nickel Nanowires: Synthesis, Characterization and Application as Effective Catalysts for the Reduction of Nitroarenes. *Catalysts*. 8(11), 566.

References

1. Gladkov, S.O., Bogdanova, S.B. (2015) To the theory of the Landau-Lifshitz-Hilbert equation. *Phys. Solid State* 57(5), 929–932 (in Russian).

2. J. Vishal, A. Sethi, D-K. Kumar. (2013) Finite Element Method: An Overview. *Walailak Journal of Science and Technology*. 10(1), 1–8.

3. T. Wasiak, L. Przypis, K. Walczak, D. Janas. (2018) Nickel Nanowires: Synthesis, Characterization and Application as Effective Catalysts for the Reduction of Nitroarenes. *Catalysts*. 8(11), 566.

Сведения об авторах

Шарейко М.В., аспирант кафедры микро- и наноэлектроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Данилюк А.Л., к.ф.-м.н., доцент, доцент кафедры микро- и наноэлектроники, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», danilyuk@bsuir.by.

Information about the authors

Shareiko M.V. graduate student at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”.

Danilyuk A.L., Cand. of Sci., Associate Professor, Associate Professor at the Department of Micro- and Nanoelectronics, Educational Institution “Belarusian State University of Informatics and Radioelectronics”, danilyuk@bsuir.by.

UDC 004.056:336.71(076)

TECHNICAL MEANS OF INFORMATION PROTECTION

Zihan Huang

Educational Institution “Belarusian State University of Informatics and Radioelectronics”, Minsk, Republic of Belarus

Abstract. The article discusses modern technical means of information protection, including hardware and software-hardware complexes. A classification is provided, along with the operating principles and examples of implementing systems designed to counter unauthorized access, technical channel leakage, and malicious impacts. A method for personal data protection based on the identifiers introducing is proposed, which enhances the security of identification and authentication processes. Special attention is paid to the certification and effectiveness of applying such means in critical information systems.

Keywords: technical information protection; information security means; unauthorized access; firewalls; intrusion detection system; cryptographic gateway; biometric

authentication; identifiers introducing; personal data protection; security tools certification; information leakage; malware protection.

Introduction

The current stage of development of the information society is characterized by the growing role of information as a key strategic resource. At the same time, the number of threats aimed at violating the confidentiality, integrity, and availability of information is increasing. Technical means of information protection play a central role in building a comprehensive information security system. They include a wide range of devices, systems, and complexes designed to protect information processed, stored, and transmitted in automated systems. The relevance of this topic is confirmed by the steady growth of cyberattacks, the complexity of modern malicious software, and the tightening of regulatory requirements for information protection in critical infrastructure facilities. The purpose of this work is to analyze the current state, classification, and features of the application of technical means of information protection, with a focus on modern methods for personal data protection based on identifiers introducing.

Main Part

Modern technical means of information protection can be classified according to their functional purpose, method of implementation, and level of protection provided. Based on their functional purpose, the following main classes are distinguished: means of protection against unauthorized access, means of protecting against information leakage through technical channels, means of cryptographic information protection, and means of security monitoring and analysis.

An example of the figure design and the caption to it is presented below. Figure shows a generalized structural diagram of interaction between various technical means of information protection within a corporate information system.

Among the promising approaches to enhancing personal data security, the method based on identifiers introducing deserves special attention. This method involves the generation and assignment of unique identifiers to data subjects and their personal data attributes, enabling fine-grained access control and traceability. The core principle is to replace direct personal identifiers with derived identifiers that are used throughout the system, thereby reducing the risk of unauthorized correlation and disclosure.

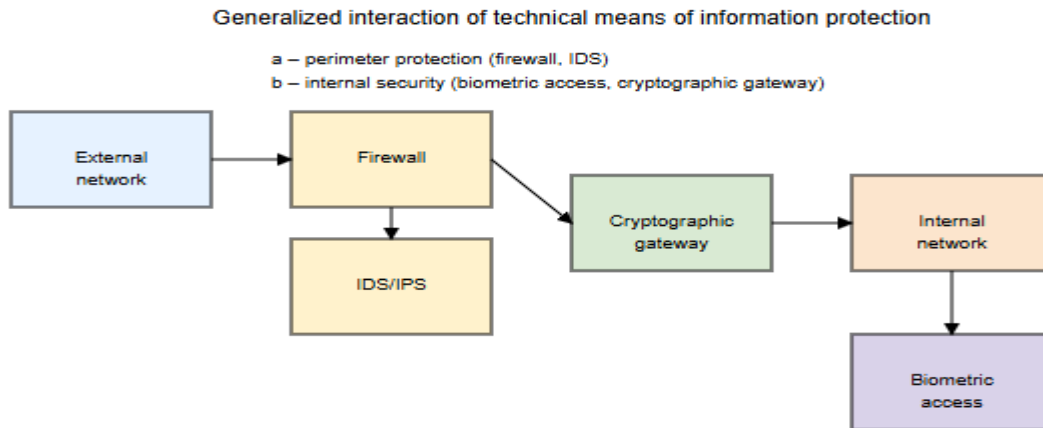


Figure capture: a – perimeter protection (firewall, intrusion detection system);
b – internal security (biometric access control, cryptographic gateway)

The effectiveness of the identifiers introducing method can be evaluated by the reduction in the probability of successful re-identification. The probability that an attacker successfully links a set of actions to a specific data subject is given by:

$$P_{reid} = P_{initial} * (1 - R_{id}), \quad (1)$$

where P_{reid} – the probability of successful re-identification; $P_{initial}$ – the probability of re-identification without identifier transformation; R_{id} – the reduction coefficient achieved through identifier introducing ($0 \leq R_{id} \leq 1$). As R_{id} approaches 1, the risk of re-identification approaches zero.

Examples of equation design are provided below. To assess the effectiveness of technical protection means, one can use the probability of overcoming protection as a key indicator. The total probability of unauthorized access when sequentially overcoming n protection lines is determined by the formula:

$$P_{total} = 1 - \prod_{i=1}^n (1 - P_i), \quad (2)$$

where P_{total} – the total probability of unauthorized access; P_i – the probability of overcoming the i -th line of defense; n – the number of lines of defense. This expression demonstrates that increasing the number of independent lines of defense significantly reduces the overall probability of a successful attack.

An example of table design is presented below. A comparative analysis of the main technical means of information protection is provided in Table including the identifiers introducing method as a supplementary control.

Comparative characteristics of technical means of information protection

Type of means	Function	Implementation	Certification requirement
Firewall	Network traffic filtering	Hardware and software	Mandatory
Intrusion detection system	Attack detection	Software and hardware	Mandatory
Cryptographic gateway	Data encryption	Hardware and software	Mandatory
Biometric authentication	Identity verification	Hardware and software	For critical systems
Identifiers introducing method	Personal data protection, traceability	Software	Recommended for personal data systems
Security scanner	Vulnerability assessment	Software	Recommended

Conclusion

Technical means of information protection are a key element of modern information security systems. The analysis showed that the most effective is a comprehensive approach combining perimeter protection tools, cryptographic protection, biometric access control systems, and advanced methods for personal data protection such as the identifiers introducing method. The identifiers introducing method provides enhanced protection for personal data by substituting direct identifiers with derived ones, significantly reducing the risk of re-identification and unauthorized access. A promising direction for further development is the integration of artificial intelligence methods for behavioral analysis of users and detecting anomalies, as well as the transition to import-independent technical protection means in critical sectors. The development and implementation of effective technical protection means require constant updating of approaches in accordance with the dynamics of threats.

References

1. Comprehensive Approach to Designing Technical Information Protection Systems
2. Modern Intrusion Detection Systems: Architectures and Effectiveness
3. Guidelines on Certification of Technical Information Protection Means
4. Application of Cryptographic Gateways in Corporate Networks
5. Dynamic Identifier-Based Protection Framework for Personal Data in Distributed Systems
6. Methods of Making Management Decisions

Information about the author

Zihan Huang, master student of Educational Institution “Belarusian State University of Informatics and Radioelectronics”, e-mail: 1913017013@qq.com.

УДК 004.056:378.016

ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В.В. Золотов

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматриваются актуальные вопросы подготовки специалистов в области защиты информации. Анализируется разрыв между фундаментальными знаниями, изложенными в классических трудах (В.Ф. Шаньгин), и современными требованиями к практическим навыкам выпускников. На основе исследований последних лет (Д.П. Зегжда, С.С. Корт) обосновывается необходимость внедрения в учебный процесс активных методов обучения, включая моделирование угроз и решение практических задач. Предложены пути интеграции фундаментальной подготовки и практико-ориентированного обучения

Ключевые слова: информационная безопасность; подготовка кадров; профессиональные компетенции; высшее образование; киберугрозы; учебный план; моделирование угроз; практико-ориентированное обучение; формирование навыков; киберполигоны.

FORMATION OF PROFESSIONAL COMPETENCIES OF INFORMATION SECURITY SPECIALISTS

V.V. Zolotov

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article deals with topical issues of training specialists in the field of information security. The gap between the fundamental knowledge presented in classical works (V.F. Shangin) and modern requirements for graduates' practical skills is analyzed. Based on recent research (D.P. Zegzhda, S.S. Kort), the necessity of introducing active learning methods, including threat modeling and solving practical problems, into the educational process is substantiated. Ways to integrate fundamental training and practice-oriented learning are proposed.

Keywords: information security; personnel training; professional competencies; higher education; cyber threats; curriculum; threat modeling; practice-oriented learning; skills formation; cyber ranges.

Введение

Современный этап развития информационного общества характеризуется стремительным ростом количества и сложности киберугроз. В этих условиях качество подготовки специалистов по защите

информации становится критическим фактором обеспечения национальной безопасности любого государства. Однако система высшего образования сталкивается с серьезным вызовом: с одной стороны, необходимо дать студентам фундаментальные знания, без которых невозможно понимание основ информационной безопасности, с другой – подготовить выпускника, способного сразу после окончания вуза решать реальные практические задачи. Целью данной работы является анализ существующих подходов к подготовке кадров в области защиты информации и определение путей совершенствования образовательных программ на основе интеграции фундаментальных знаний и современных практико-ориентированных методик.

Основная часть

Фундаментальной основой подготовки специалистов по защите информации являются классические труды, среди которых особое место занимает учебник В.Ф. Шаньгина «Информационная безопасность и защита информации». В нем изложены базовые принципы комплексной системы защиты информации, включая обеспечение конфиденциальности, целостности и доступности данных, а также архитектура защищенных систем и организационно-правовые аспекты. Однако, как показывают исследования последних лет, одного фундаментального образования недостаточно. В работе Д.П. Зегжды с соавторами доказывалось, что наибольшую эффективность демонстрирует обучение, построенное на активном вовлечении студентов в решение практических задач, в частности через моделирование угроз, когда студенты самостоятельно строят модели нарушителя и разрабатывают меры противодействия.

С.С. Корт развивает эту мысль, указывая на необходимость создания в вузах киберполигонов – программно-аппаратных комплексов, имитирующих реальную информационную инфраструктуру, где студенты отрабатывают навыки обнаружения и отражения атак. Такой подход формирует профессиональные компетенции – способность применять знания в реальных ситуациях. Еще одним важным аспектом является обучение управлению информационными рисками. Как отмечает А.М. Астахов, специалист должен понимать не только техническую, но и экономическую сторону: обосновывать необходимость средств защиты и оценивать эффективность инвестиций в безопасность. Таким образом, оптимальная модель подготовки специалиста представляет собой синтез трех компонентов: фундаментальной теоретической подготовки (Шангин В.Ф.), практической отработки навыков на киберполигонах и в ходе моделирования угроз (Зегжда Д.П., Корт С.С.), а также изучения вопросов управления рисками и экономики безопасности (Астахов А.М.).

Information about the authors

Проведенный анализ позволяет сделать вывод о необходимости модернизации образовательных программ по направлению «Информационная безопасность». Классическая фундаментальная подготовка, представленная трудами В.Ф. Шаньгина, остается необходимой основой, однако она должна быть дополнена современными практико-ориентированными методиками, описанными в работах Зегжды Д.П., Корта С.С. и Астахова А.М. Только сочетание глубоких теоретических знаний и устойчивых практических навыков, сформированных в процессе активного обучения, позволит готовить специалистов, способных эффективно противостоять современным киберугрозам. Перспективным направлением дальнейших исследований является разработка конкретных методик интеграции киберполигонов в учебный процесс и создание системы оценки сформированности профессиональных компетенций.

Список использованных источников

1. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – 3-е изд., перераб.
2. Зегжда, Д.П. Подход к формированию профессиональных компетенций в области информационной безопасности на основе активных методов обучения / Д.П. Зегжда, А.Н. Ковтун, Е.Ю. Павленко // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 45-54.
3. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК Пресс, 2022. – 320 с.
4. Корт, С.С. Теоретические основы подготовки специалистов по защите информации в условиях цифровой трансформации / С.С. Корт // Безопасность информационных технологий. – 2024. – Т. 31, № 1. – С. 92-103

References

1. Shangin, V.F. Information Security and Information Protection / V.F. Shangin. – 3rd ed., revised and updated. – Moscow: DMK Press, 2020. – 702 p.
2. Zegzhda, D.P. Approach to the Formation of Professional Competencies in the Field of Information Security Based on Active Learning Methods / D.P. Zegzhda, A.N. Kovtun, E.Y. Pavlenko // Cybersecurity Issues. – 2023. – No. 4(56). – P. 45-54.
3. Astakhov, A.M. The Art of Information Risk Management / A.M. Astakhov. – Moscow: DMK Press, 2022. – 320 p.
4. Kort, S.S. Theoretical Foundations of Training Information Security Specialists in the Context of Digital Transformation / S.S. Kort // Information Technology Security. – 2024. – Vol. 31, No. 1. – P. 92-103.

Сведения об авторе

Золотов В.В., курсант учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», e-mail: vadimzolotov94@gmail.com.

Information about the author

Zolotov V.V., cadet of Educational Institution "Belarusian State University of Informatics and Radioelectronics", e-mail: vadimzolotov94@gmail.com.

УДК 004.056

СРЕДСТВО ПРОГРАММНОЙ ЗАЩИТЫ ОТ HID-АТАК BADUSB

А.А. Лебедев

УО «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Рассматривается проблема атак через USB-устройства, эмулирующие клавиатуру, которые не детектируются традиционными антивирусными средствами. Разработан метод активной защиты, основанный на анализе поведения подключаемых устройств в реальном времени. Описана архитектура программного решения, включающая три этапа: мгновенное обнаружение, поведенческий анализ и интеллектуальную блокировку. Приведены результаты экспериментальной проверки эффективности метода.

Ключевые слова: BadUSB; уязвимость; манипуляция; защита информации; поведенческий анализ; USB-устройства; активная блокировка.

SOFTWARE PROTECTION AGAINST BADUSB HID-ATTACKS

A.A. Lebedev

*Belarusian state university of informatics and radioelectronics
Minsk, Republic of Belarus*

Abstract. The problem of attacks via USB devices that emulate a keyboard, which are not detected by traditional antivirus tools, is being considered. A method of active protection based on the analysis of the behavior of connected devices in real time has been developed. The architecture of the software solution is described, which includes three stages: instant detection, behavioral analysis and intelligent blocking. The results of an experimental verification of the effectiveness of the method are presented.

Keywords: BadUSB; vulnerability; data; manimulation; information protection; behavioral analysis; USB devices; active blocking.

Введение

Рост числа кибератак с использованием специализированных USB-устройств, эмулирующих клавиатуру (BadUSB), представляет серьезную угрозу для информационных систем. Устройства, стоимостью от 50 рублей, подключаются к компьютеру и в течение нескольких секунд

выполняют predetermined скрипт, который может включать кражу паролей, установку вредоносного ПО, модификацию системных настроек или вывод системы из строя. Традиционные антивирусы бессильны против подобных атак, поскольку устройство идентифицируется операционной системой как легитимная клавиатура, а вредоносные действия выполняются на уровне ввода. Существующие методы защиты (ограничение USB-портов, фильтрация типов устройств, аппаратные USB-концентраторы) либо снижают функциональность системы, либо не обеспечивают достаточного уровня защиты от атак, начинающихся сразу после подключения. В данной работе предлагается метод активной защиты, основанный на анализе поведения устройства в реальном времени. Разработанное программное решение USB-Shield позволяет детектировать вредоносную активность на ранней стадии и мгновенно блокировать подозрительное устройство.

Основная часть

BadUSB-устройства (например, Arduino Leonardo, Rubber Ducky) подключаются к USB-порту и эмулируют клавиатуру. Операционная система автоматически инициализирует драйвер HID-клавиатуры, после чего устройство начинает ввод предварительно запрограммированных команд со скоростью, достигающей 1000 символов в секунду. Типичный сценарий атаки занимает 3–5 секунд и может включать: открытие командной строки, загрузку и выполнение вредоносного скрипта, извлечение сохраненных паролей, создание скрытых учетных записей.

Разработанный метод базируется на анализе поведения подключаемого устройства на трех уровнях: физическом, поведенческом и операционном. Реализация выполнена на языке C++ с использованием Windows API, что обеспечивает минимальное потребление ресурсов и высокую скорость реакции.

Этап 1 - Мгновенное обнаружение. Система постоянно мониторит подключение новых USB-устройств. Обнаружение нового устройства инициирует защитный протокол. Время реакции на этом этапе составляет менее 200 мс.

Этап 2 - Поведенческий анализ. После обнаружения устройства запускается анализатор, который проверяет идентификатор устройства на соответствие списку известных вредоносных (например, VID/PID Arduino). После этого измеряет скорость ввода (при превышении определенного количества символов в секунду устройство считается подозрительным). Одновременно с этим распознает последовательности команд, характерные для вредоносных скриптов (более 50 паттернов, включая запуск командных оболочек, изменение реестра, сетевые команды и др.)

Для повышения точности анализа используются как заводские, так и настраиваемые пользователем паттерны через файл конфигурации.

Этап 3 - Блокировка. При выявлении признаков вредоносной активности выполняются следующие действия. Экстренный сброс фокуса ввода на рабочий стол для предотвращения дальнейшего ввода. Блокировка дальнейшего ввода с устройства с помощью низкоуровневого хука клавиатуры. Отключение устройства и удаление его из системы через системные API. Ведение детального журнала событий.

Экспериментальная проверка. Эффективность метода оценивалась на тестовой системе с использованием Arduino Leonardo, настроенного на выполнение типового вредоносного скрипта (открытие командной строки, кража пароля от wifi сети, копирование файлов). Проведено 10 запусков атаки на компьютере под управлением Windows 10 с установленным USB-Shield. Результаты:

Время реакции: в среднем 280 мс (от подключения до блокировки устройства). Эффективность блокировки: 9 из 10 атак были прерваны до выполнения вредоносных команд. Один пропуск связан с особенностью работы драйверов HID при очень высокой скорости ввода, что потребовало дополнительной оптимизации. Ложные срабатывания: зафиксировано 0 ложных срабатываний при использовании легитимных клавиатур, мышей и флеш-накопителей. Для сравнения, те же атаки против стандартных антивирусов прошли успешно в 100 % случаев, поскольку антивирус не обнаружил вредоносных файлов.

Заключение

В работе предложен метод активной защиты от атак BadUSB, основанный на поведенческом анализе. Реализованное программное решение продемонстрировало высокую эффективность в условиях реальных атак, при этом не оказывая заметного влияния на производительность системы. Дальнейшее развитие планируется в направлении расширения базы поведенческих паттернов, интеграции с корпоративными системами управления и поддержки других классов USB-устройств (например, эмуляция сетевых карт).

Сведения об авторе

Лебедев А. А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexandercorp77@gmail.com.

Information about the author

Lebedev A. A., student, faculty of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexandercorp77@gmail.com.

ДЛЯ ЗАМЕТОК

[illegible]

[illegible]

Научное издание

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Материалы
XXIV Международной научно-технической конференции
(Республика Беларусь, Минск, 8 апреля 2026 года)

В авторской редакции
Ответственный за выпуск *О. В. Бойправ*
Компьютерная верстка *В. С. Мокеров*

Подписано в печать 17.04.2026. Формат 60×84 1/8. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 50,92. Уч.-изд. л. 28,1. Тираж 50 экз. Заказ 52.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/238 от 24.03.2014,
№ 2/113 от 07.04.2014, № 3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск