Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК [537.531:621.762]:004.056

ГОНДАГ САЗ
Мостафа Мохаммад

МОДЕЛИ И АЛГОРИТМЫ АВТОМАТИЗИРОВАННОГО ВЫБОРА И ОРГАНИЗАЦИИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ФИНАНСОВЫХ УЧРЕЖДЕНИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.01 – Системный анализ, управление и обработка информации, 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск, 2021

Научная работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**Вишняков Владимир Анатольевич**, доктор технических наук, профессор, профессор кафедры инфокоммуникационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Официальные оппоненты:	**Дудкин Александр Арсентьевич**, доктор технических наук, профессор, заведующий лабораторией государственного научного учреждения «Объединенный институт проблем информатики Национальной академии наук Беларуси»
	Захаров Владимир Владимирович, кандидат технических наук, доцент, доцент кафедры интеллектуальных информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Оппонирующая организация:	Белорусский национальный технический университет

Защита состоится «18» марта 2021 г. в 14.00 на заседании совета по защите диссертаций Д 02.15.01 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «___» февраля 2021 г.

Ученый секретарь совета
по защите диссертаций,
кандидат технических наук, доцент М. П. Ревотюк

ВВЕДЕНИЕ

Общая тенденция развития интеллектуальных и информационных технологий показывает, что модели и средства обработки информации на их основе получают все большее развитие и распространение в информационном управлении как для работы юридических, так и физических лиц. Этому способствует развитие сетевого корпоративного управления, интеллектуализация бизнеса, исследования в области обработки знаний с использованием автоматизированного выбора.

При большом многообразии работ в области идентификации и аутентификации пользователей актуальным является исследование вопросов безопасной работы пользователя мобильных приложений в облачной среде. Выбор модели аутентификации пользователей в конкретных условиях информационной безопасности, особенно в корпоративных информационных системах финансовых учреждений (КИС ФУ) с облачными вычислениями и мобильными приложениями, не до конца разработан, что требует дальнейших исследований. Особый интерес представляют модели и алгоритмы выбора модели аутентификации пользователей в КИС ФУ в среде облачных вычислений при работе с мобильными приложениями с использованием технологии представления и обработки знаний, которые и обусловливают актуальность исследований в диссертационной работе.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Тема диссертационной работы утверждена приказом ректора учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» № 658-О от 29.12.2014 и соответствует подразделу 5 «Информатика и космические исследования» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2016 – 2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12.03.2015 № 190.

Диссертационное исследование выполнялось в рамках НИР: «Модели и средства информационного управления и электронного маркетинга предприятия» № ГР 20115472 от 22.12.2011; «Новые технологии в информационном управлении и электронном маркетинге предприятий» № ГР 20162078 от 22.04.2016.

Цель и задачи исследования

Цель диссертационной работы – разработка базы моделей, алгоритмов и средств выбора и организации аутентификации пользователей мобильных приложений в интегрированных корпоративных информационных системах

финансовых учреждений (ИКИС ФУ) с автоматизацией параметрического выбора варианта аутентификации.

Для достижения поставленной цели решались следующие задачи:

1. Проведение анализа литературных и электронных источников выбора и организация аутентификации пользователей в ИКИС ФУ с использованием облачных вычислений.
2. Разработка символьных моделей аутентификации пользователей мобильных приложений для формирования базы знаний в ИКИС ФУ.
3. Разработка методики автоматизированного выбора и организация аутентификации пользователей мобильных приложений в ИКИС ФУ.
4. Разработка алгоритма параметрического выбора модели аутентификации с использованием знаний для пользователей мобильных приложений в ИКИС ФУ.
5. Разработка выбранных алгоритмов аутентификации пользователей мобильных приложений в ИКИС ФУ.
6. Программная реализация и апробирование методики, алгоритма параметрического выбора модели аутентификации пользователей мобильных приложений в ИКИС ФУ.
7. Программная реализация и апробирование алгоритмов аутентификации пользователей мобильных приложений в ИКИС ФУ.

Научная новизна

1. Разработаны модели символьного описания методов аутентификации пользователей мобильных приложений в ИКИС финансовых учреждений, отличающиеся от известных описаний возможностью создания базы знаний, что позволило сформировать основу для дальнейшего автоматизированного принятия решения по выбору модели аутентификации в конкретной ситуации информационной безопасности.
2. Предложена методика выбора варианта модели аутентификации пользователей мобильных приложений на основе базы знаний и поддержки параметрического принятия решений для ИКИС финансовых учреждений, отличающаяся от известных методик учетом факторов информационной безопасности, ответов администратора по оценке информационной безопасности, что позволило сократить время принятия решения по выбору варианта аутентификации клиента мобильных приложений.
3. Разработан алгоритм параметрического выбора модели аутентификации для пользователей мобильных приложений в ИКИС финансовых учреждений, отличающийся от известных интуитивных подходов принятия решений администратором сети, что обеспечило автоматизированный выбор метода аутентификации.

4. Разработаны алгоритмы аутентификации пользователей мобильных приложений и их программная реализация в ИКИС с облачной средой финансовых учреждений, что вместе с автоматизированным выбором метода аутентификации позволило повысить значение интегрированного показателя информационной защиты финансовой организации на 10,5 %.

Положения, выносимые на защиту

1. Модели символьного описания методов аутентификации пользователей мобильных приложений в ИКИС финансовых учреждений, на основе которых формируется база знаний моделей для дальнейшего автоматизированного принятия решения о выборе варианта аутентификации в конкретной ситуации информационной безопасности.

2. Методика автоматизированного выбора варианта модели аутентификации пользователей мобильных приложений на основе базы знаний моделей для ИКИС финансовых учреждений, которая поддерживает параметрическое принятие решений, что в отличие от известных подходов позволяет сократить время принятия решения по выбору модели аутентификации клиентов мобильных приложений и повысить интегральный показатель системы защиты финансового учреждения в работе пользователей.

3. Алгоритм параметрического выбора модели аутентификации для пользователей мобильных приложений в ИКИС финансовых учреждений и его программная реализация, позволяющие администратору выбрать вариант модели аутентификации с использованием автоматизированного средства.

4. Алгоритмы выбранных моделей аутентификации для пользователей мобильных приложений в ИКИС финансовых учреждений и их программная реализация вместе с автоматизированным средством выбора аутентификации, позволяющие получить повышение интегрированной оценки информационной защиты финансовой организации на 10,5 %.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании цели и задач исследования, разработке моделей, алгоритмов, программной реализации, участие в проведении экспериментов по их исследованию, а также в обработке, анализе и интерпретации полученных результатов, формулировке основных выводов. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем д-м техн. наук, профессором В. А. Вишняковым.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: научно-практическом семинаре «Проблемы информационного управления», Минск, (МИУ 2016–2017); 5-й и 7-й Международных научно-технических конференциях OSTIS- 2015, OSTIS-2017 БГУИР (Минск, 2015, 2017); XIII–XV Белорусско-российских НТК «Технические средства защиты информации», БГУИР (Минск, 2015–2017); XX-XIV Международных научно-технических конференциях «Современные средства связи» (Минск, 2015–2019); на Международном научно-техническом семинаре «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных» (Минск, БГУИР 2019).

Разработанные модели и средства информационного управления аутентификацией пользователей мобильных приложений в ИКИС использованы в корпоративной сети банка ЗАО «Н.Е.Б. Банк», учебном процессе Минского инновационного университета, при выполнении НИР в лаборатории «Информационного управления» МИУ.

Опубликование результатов диссертации

По результатам выполненных исследований, представленных в диссертации, опубликовано 18 научных работ, в том числе 5 статей в рецензируемых научных журналах, рекомендованных ВАК для опубликования результатов научных исследований, 3 статьи в материалах сборников международных научно-технических конференций и семинаров, 10 тезисов докладов. Общий объем публикаций по теме диссертации, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, составляет 3,9 авторского листа.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с выводами по каждой главе, заключения, библиографического списка и приложений.

Общий объем диссертационной работы составляет 109 страниц, из них 73 страниц текста, 43 рисунка на 14 страницах, 8 таблиц на 3 страницах, библиографический список из 112 источников на 10 страницах, включая 18 собственных публикаций автора на 2 страницах, 4 приложения на 9 страницах.

ОСНОВНАЯ ЧАСТЬ

Во **введении** определены основные направления проводимых исследований, их актуальность, показана необходимость их осуществления.

В **первой главе** на основании анализа литературных данных и электронной информации показано, что для организации аутентификации пользователей существует много подходов, методов и средств. Наибольшие результаты в проблему аутентификации и идентификации внесли три организации: RSA Laboratories, Microsoft, Facebook.

Организация защиты и аутентификации пользователей в средах облачных вычислений (ОВ) имеет специфику, а именно: защита периметра и разграничение сети; динамичность виртуальных машин (ВМ); уязвимости и атаки внутри виртуальной среды; защищенность данных и приложений; доступ системных администраторов к серверам и приложениям; защита не работающих ВМ. Предложены следующие решения для среды ОВ: шифрование, защита данных при передаче, изоляция пользователей. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service).

Проанализированы различные модели аутентификации пользователей. Модель обезличивания персональных данных (ПД) обладает свойством универсальности, поскольку может быть использована для обезличивания разных наборов данных, и является расширяемой за счет возможности добавления новых параметров. Метод формирования эталонов идентифицируемых образов в пространстве малоинформативных признаков, основанный на построении плотностей распределения вероятностей используемых признаков с последующим преобразованием полученных распределений в компактные кластеры на основе алгоритма нечеткого вывода, позволяет уменьшить количество ошибок при идентификации пользователей компьютерных систем по динамике подсознательных движений в среднем в 1,6 раза. Математическая модель социальной идентификации позволяет по заданному числу неудовлетворительных оценок вычислить вероятность успешной идентификации с использованием метода вычисления времени премодерации.

Гарантии аутентификации пользователей за рубежом были разделены на 4 уровня по конфиденциальности идентификационных данных: отсутствие требований, средний уровень требований, высокий уровень требований и очень высокий.

Проанализированы способы аутентификации пользователей в мобильных приложениях: по паролю (с передачей хеш-пароля, с единственным входом (Single Sign-On)), сертификатам, одноразовым паролям, ключам доступа, токенам.

Рассмотрено несколько форматов токенов для веб-приложений. Вместе с тем, практика выбора модели аутентификации базируется на интуитивном экспертном подходе и нуждается в автоматизации. Для автоматизированного выбора модели аутентификации могут использоваться базы знаний, продукционные правила, онтологии. На основе проведенного анализа сформулированы цель и задачи диссертации.

Вторая глава включает систематизацию описания моделей выбора и организации аутентификации пользователей ИКИС с элементами ОВ, в том числе для мобильных приложений в ИКИС для формирования базы знаний, которая будет использоваться для выбора лучшей модели.

Модели аутентификации пользователей в среде облачных вычислений описаны с использованием символьного подхода. В статьях [4, 7] представлены элементы описания для аутентификации работы пользователей в среде ОВ. Участники взаимодействий следующие: пользователь (пользователями могут быть физические лица и организации), аутентификатор подлинности (Trusted Authenticator − TA), облачный провайдер услуг (Cloud Service Provider − CSP), цифровая подпись (Digital Signature − DS), агент CSP's. Ниже представлены функции элементов данного подхода:

1. Пользователь имеет ограниченный доступ к услугам из облака предлагаемых услуг, он запрашивает облачные ресурсы у CSP's.

2. TA устанавливает соединение и доверительные отношения с органом аутентификации. Задача TA в облачной среде − обеспечить пользователю безопасный доступ к облачным сервисам через поставщика услуг.

3. CSP может динамически масштабироваться для удовлетворения потребностей пользователей, потому что поставщик услуг предоставляет необходимое для обслуживания оборудование и программное обеспечение.

4. DS является электронной подписью, которая идентифицирует личность отправителя сообщения или подписавшего документ и удостоверяет, что оригинальное содержание посланного сообщения или документа не изменилось.

5. Агент CSP's способен принимать решения на выполнение задач от имени своих пользователей. Агенты имеют право взаимодействовать с другими агентами путем переговоров, сотрудничества и координации. В CSP агент работает для предоставления услуг, обслуживания переговоров, услуг сотрудничества и их координации.

Представим описание моделей аутентификации пользователей с использованием алгебры объектов, введя обозначения: X − пользователь, Y – сервер подлинности, t_x, − временная метка; r_x, r_y – случайные числа для X и Y соответственно; S_x, S_y − подписи, сгенерированные X и Y; Cox, Coy − сертификаты открытого ключа для X и Y. Приведем варианты символьных моделей аутентификации пользователей мобильных приложений [4]:

1. Односторонняя аутентификация пользователей с применением меток времени имеет вид:

$$X \rightarrow Y\text{: } Cox,\ t_x,\ I_x, S_x(t_x,\ I_x). \quad (1)$$

После принятия сообщения сервер подлинности проверяет правильность метки времени t_x, полученный идентификатор I_x и, используя открытый ключ из сертификата Cox, корректность цифровой подписи $S_x(t_x,\ I_x)$.

2. Односторонняя аутентификация пользователей с применением случайных чисел:

$$Y \rightarrow X,\ r_y\ ; \quad X \rightarrow Y\text{: } Cox,\ r_x,\ I_y,\ \mathrm{S_x}(r_x, r_y,\ I_x). \quad (2)$$

Сервер подлинности Y направляет пользователю X случайное число r_y, на основании сообщения от X. Используя открытый ключ X из сертификата Cox, Y проверяет корректность подписи $S_x(r_x,\ r_y,\ I_x)$ под числом r_x, числом r_y, полученными в первом сообщении, и его идентификатором I_x.

3. Двухсторонняя аутентификация с применением случайных чисел:

$$Y \rightarrow X,\ r_y\ ;\ X \rightarrow Y,\ Cox,\ r_x,\ I_y,\ S_x(r_x,\ r_y,\ I_x);\ Y \rightarrow X\text{: } Coy,\ I_x,\ S_y(r_x, r_y,\ I_x). \quad (3)$$

В этой модели обработка первой и второй частей выполняется, как в (1), а третья часть обрабатывается аналогично (2).

4. Модель аутентификации по паролю с сервером приложений основывается на том, что пользователь должен предоставить серверу приложений имя − U_n и пароль − P_s для успешной идентификации и аутентификации в системе.

Опишем эту модель: пусть X − пользователь, B − браузер, S_p − сервер приложений, A − признак аутентифицирован, n − уникальное значение, H − хеш-функция, C − процесс шифрования, P_k − k-е приложение. Тогда базовая модель аутентификации будет иметь вид:

$$X(U_n,\ P_s) \rightarrow B \rightarrow S_p; \quad S_p(A) \rightarrow B \rightarrow X. \quad (4)$$

Вторая разновидность для этой модели отличается от базовой (данные U_n, P_s передаются в открытом виде), зашифрованным вариантом (модель с шифрованием), выглядит так:

$$X\,(C(U_n),\ P_s(U_n)) \rightarrow B \rightarrow S_p; \quad S_p(A) \rightarrow B \rightarrow X. \quad (5)$$

Третьей разновидностью является двухсторонняя модель с использованием хеш-функции, когда сервер приложений посылает браузеру уникальное значение n, браузер передает значение хеш-пароля пользователя, вычисленное с использованием указанного n. Она имеет вид:

$$X \rightarrow B \rightarrow S_p;\ S_p(n) \rightarrow B \rightarrow X;\ X(U_n,\ H(n,\ P_s) \rightarrow B \rightarrow S_p;\ S_p(A) \rightarrow B \rightarrow X. \quad (6)$$

5. Модель аутентификации по форме приложения основывается на том, что пользователь должен предоставить приложению имя − U_n и пароль − P_s. Для успешной аутентификации запишем ее вид:

$$X\,(U_n, P_s) \rightarrow B \rightarrow P_k\,(S_p);\;\; P_k\,(S_p(A)) \rightarrow B \rightarrow X. \qquad (7)$$

6. В модели аутентификации пользователей по сертификату введем сервер аутентификации − SA, сертификат пользователя − $C_a(k)$, включающий k атрибутов и подписанный SA − $C_a(k, SA)$, секретный ключ – Ks. Модель имеет вид:

$$X(C_a(k), Ks) \rightarrow SA;\; SA(C_a(k, SA) \rightarrow X;\; X(C_a(k, SA) \rightarrow S_p;\; S_p \rightarrow SA;\; S_p(A) \rightarrow B \rightarrow X. \qquad (8)$$

Модель более надежная, однако, трудности с распространением и поддержкой сертификатов делают ее сложно реализуемой.

7. Аутентификация пользователей по одноразовым паролям (ОП) обычно применяется дополнительно по другим параметрам для реализации двухфакторной аутентификации (two-factor authentication − 2FA). Наличие двух факторов позволяет увеличить уровень безопасности, что востребовано для определенных видов финансовых веб-приложений (перевод денег, изменение настроек, паролей и т. д.). Введем токен T, который может быть получен на основании секретного ключа, текущего времени − t и запроса одноразового пароля − R. Модель ОП представляется в виде:

$$X(U_n, P_s) \rightarrow B \rightarrow P_k\,(S_p);\;\; P_k\,(S_p, R\,) \rightarrow X;\; X(T(Ks, t))) \rightarrow B \rightarrow P_k\,(S_p). \qquad (9)$$

8. Модель аутентификации пользователей по ключам доступа используется для определения устройств, сервисов или других приложений при обращении к веб-сервисам − WS, хранящихся на облачном сервере − S_{ws}, средством аутентификации является ключ доступа − K_a (произвольная строка символов, генерируемая сервером S_{ws}). Модель имеет вид:

$$X\,(U_n, P_s) \rightarrow B \rightarrow S_{ws};\; S_{ws}(K_a) \rightarrow X;\;\; X\,(K_a) \rightarrow P_k\,(S_{ws}). \qquad (10)$$

Более сложная модель аутентификации по ключам для незащищенных соединений включает два ключа: открытый − K_o и секретный − K_s. K_o используется для идентификации клиента, K_s позволяет сгенерировать цифровую подпись. Эта модель имеет вид:

$$X\,(K_o) \rightarrow B \rightarrow S_{ws};\;\; S_{ws}\,(n) \rightarrow B \rightarrow X;\;\; X\,(H(n, K_s) \rightarrow B \rightarrow S_{ws.} \qquad (11)$$

Сервер S_{ws} после установки соединения посылает клиенту уникальное значение n, а клиент возвращает хеш этого значения, вычисленный с использованием K_s. Это позволяет избежать передачи всего ключа в оригинальном виде.

Модель аутентификации пользователей по *токенам* применяется при построении распределенных систем *Single Sign-On* (SSO), где одно приложение − *SP* (Service Provider) делегирует функцию распознавания

пользователей другому приложению − *IP* (Identity Provider) (пример − вход в приложение через учетную запись в социальных сетях). Токен $T(P_i)$ генерируется *IP*, где P_i − параметры токена. Модель имеет вид:

$$X\,(K_o)\rightarrow B\rightarrow IP;\ IP(n)\rightarrow B\rightarrow X;\ X\,(H(n, K_s)\rightarrow B\rightarrow IP;\ IP(T\,(P_i))\rightarrow X;\ X(T\,(P_i))\rightarrow SP. \quad (12)$$

Предложенный автоматизированный выбор моделей идентификации (МИ) и аутентификации (МА) пользователей базируется на использовании продукционных правил [4, 7]. Процесс аутентификации пользователей состоит из последовательно выполняемых процедур двух классов: к первому относятся процедуры регистрации нового пользователя ИС и хранения аутентификационной информации (АИ), ко второму – процедуры предъявления АИ, протоколы обмена «претендент – проверяющая сторона», валидации и принятия решения о результате прохождения претендентом процесса распознавания. Модель для классификации видов аутентификации представим множеством:

$$MCA = \{A, W, C\}, \quad (13)$$

где *A* − доступность (accessibility), *W* − целостность (wholeness), *C* − конфиденциальность (confidentiality).

Детализацию модели классификации выразим таким образом:

$$A = \{GA, DA, CA, PA\}: W = \{WS, WRR, WAP, WPC\}; C = \{CPP, CAP, CPC\}, \quad (14)$$

где GA − гарантия обработки запросов пользователей на аутентификацию, DA – разделение доступа пользователей, C – контроль доступа, PA − персонификация доступа, WS − целостность ПО, WRR − целостность учетных записей, WAP – целостность АИ пользователя, WPC – целостность АИ пользователя в облачной среде, CPP − конфиденциальность учетных записей, CAP − конфиденциальность АИ пользователя, CPC − конфиденциальность АИ пользователя в облачной среде.

МИ базируется на трехуровневом подходе классификации идентификаторов с семью факторами [4]: 1) как характеристик принадлежности − универсальный (*U*), корпоративный (*C*), личный (*P*); 2) для распознавания личности владельца: анонимный (*N*), персональный (*I*); 3) по доступу владельца к ресурсам: одноразовый (*O*) или многоразовый (*M*). Получаем разновидности идентификации, представленной семеркой МИ:

$$MCI = \{UNM, UPO, UPM, CNO, CNM, CPM, IPM\}, \quad (15)$$

где следующие идентификаторы: *UNM* − универсальный анонимный многоразовый (пользователь Интернета), *UPO* − универсальный персональный одноразовый (генератор одноразовых паролей), *UPM* – универсальный

персональный, содержащийся в реестре (электронный паспорт), *CNO* – корпоративный анонимный одноразовый (электронный билет), *CNM* – корпоративный анонимный многоразовый (банковская карта), *CPM* − корпоративный персональный многоразовый (смарт-карта), *IPM* − личный персональный многоразовый (биометрия).

Автоматизированный подход для выбора лучшей модели аутентификации базируется на составлении базы этих моделей, правил выбора модели в зависимости от факторов, ответов администратора об особенностях работы пользователей. На основании результатов опроса, информации базы знаний (БЗ) формируется лучший вариант аутентификации для данной ситуации.

Методика выбора модели аутентификации пользователей основана на технологии экспертных систем (рисунок 1). В базе знаний (БЗ) и базе данных (БД) будут храниться модели аутентификации, факторы их выбора, вопросы к администратору информационной безопасности (ИБ) предприятия для оценки ситуации безопасности, правила оценки моделей аутентификации по факторам, правила выбора модели аутентификации по ответам администратора. Решатель по содержимому БЗ и БД будет вычислять наиболее подходящий вид (модель аутентификации). Через интерфейс формируется БЗ, вводятся вопросы к администратору и его ответы по оценке ситуации ИБ для пользователей, для которых и определяются факторы. Решатель на основе выбранных факторов определяет лучший вид аутентификации для данной ситуации.

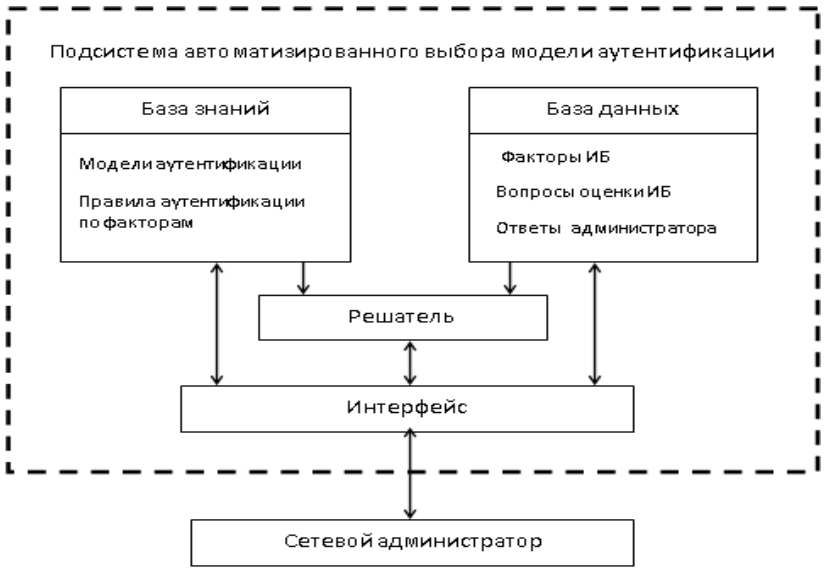

Рисунок 1. – Структура автоматизированного выбора модели аутентификации

В **третьей главе** разработан алгоритм автоматизированной системы аутентификации (АСА) выбора модели аутентификации для конкретных условий. С использованием АСА на базе символьных описаний моделей и методики (глава 2) выбирается вариант аутентификации пользователей мобильных приложений финансового учреждения, исходя из рассмотренных требований и ресурсов.

Алгоритм использует факторы, по которым будет вычисляться общая оценка модели аутентификации:

$$F = \{f_1, \dots f_{12}\},$$

где f_1 – разновидность ввода кода, f_2 – тип считывающего устройства, f_3 – стойкость, f_4 – затраты на разработку и внедрение, f_5 – трудность использования для клиента, f_6 – применимость удаленного доступа, f_7 – множественность настроек, f_8 – степень стойкости от настроек, f_9 – распространение в использовании, f_{10} – срок хранения аутентифицирующей информации, f_{11} – вероятность ошибок, f_{12} – наличие нормативной документации.

Для оценки ситуации по безопасности администратор отвечает на ряд вопросов $V = \{v_1, \dots v_N\}$. Ответы на эти вопросы включают два варианта – «Да/Нет». Далее определяем правила соответствия положительных ответов на вопросы множества V и моделей аутентификации $R = O \times A$. Шаги алгоритма:

1. Наполнение базы знаний АСА администратором.

1.1 Формирование и ввод моделей аутентификации $A = \{a_1, \dots a_5\}$,
где $a_1, \dots a_M$ – модели аутентификации.

1.2 Формирование и ввод факторов аутентификации $F = \{f_1, \dots f_k\}$.

1.3 Формирование и ввод правил соответствия моделей аутентификации и факторов $S = A \times F$.

1.4 Ввод вопросов для оценки ситуации ИБ $V = \{v_1, \dots v_N\}$.

1.5 Формулирование и ввод правил соответствия ответов на вопросы и факторов $M = O \times F$.

2. Описание и оценка ситуации по ИБ и работа системы.

2.1 Получение ответов администратора на вопросы $O = \{o_1, \dots, o_N\}$.

2.2 На основании ответов будут определены элементы множеств критериев и методов аутентификации, получена качественная оценка критериев (низкий, средний, высокий), которым поставим в соответствие количественную оценку (0, 1, 2).

3. Работает решатель, который вычисляет следующее:

3.1 Строится подмножество выбранных для сравнения факторов $F' \in F$. Данное множество F' создается на основании правил соответствия ответов на вопросы и факторов:

$$M_{ij} = O \times F,$$

где i – вопрос, j – фактор.

Если ответ o_n на вопрос v_i утвердительный, то: $o_n(v_i) = 1$, учитываем данный j фактор при выборе аутентификации.

3.2 Рекомендуемый метод аутентификации A_{bet} определяется как наибольший из подмножества методов A_p по формуле:

$A_{bet} = \max (A_p = 1/w \times \sum t_{mi}),\ i = 0,\ldots,w,$

где факторы определяются из подмножества $T \in F'$, $w -$ мощность множества T, p – текущий метод аутентификации из множества A.

4. Через интерфейс АСА администратору выводится значение $A_{bet.}$

Данный алгоритм применен для оценки наиболее приемлемых видов аутентификации пользователей мобильных приложений финансовой организации ЗАО «Н.Е.Б. Банк», в результате получена рекомендация для использования двухфакторной аутентификации. Для удобства работы организации реализована технология единого входа. Проанализированы три типа единого входа: веб-SSO, Legacy SSO и Federated SSO. Инициализация системы веб аутентификации (WebAuth) происходит до прохождения проверки подлинности доступа к защищенному ресурсу по следующему алгоритму:

1. Неавторизованный пользователь выдает запрос, пытается получить доступ к защищенному веб-ресурсу сервера приложений.

2. Сервер приложений создает запрос-токен, который шифруется с помощью публичного ключа сеанса. Пользователь перенаправляется на сервер регистрации с запросом-токеном.

3. Сервер регистрации расшифровывает запрос-маркер с помощью ключа сеанса и представляет клиенту форму входа в систему через защищенное соединение (SSL/TSL). Пользователь вводит имя пользователя, пароль и отправляет их на сервер регистрации.

4. Сервер регистрации проверяет учетные данные и генерирует два токена: прокси-токен и ID-токен. Прокси-токен сохраняется в cookie для сервера регистрации, чтобы обеспечить единый вход в будущем запросе. ID-токен отправляется обратно на сервер приложений в качестве квитанции.

5. Пользователь повторно запрашивает ресурс, располагая ID-токеном.

6. Сервер приложений проверяет ID-токен, перезаписывает его как app-токен, который будет помещен в cookie будущих запросов.

7. Для будущего доступа пользователь делает запрос с валидным app-токеном в cookie, приложение проверяет его и разрешает доступ. После успешного входа в систему Webauth SSO-опция позволяет пользователю получить доступ к другим защищенным веб-ресурсам без ввода пароля.

В сервере аутентификации для доступа пользователя к облачному веб-серверу, предоставляющего услуги пользователю, выполняется следующий алгоритм:

1. Пользователь вводит информацию для регистрации.

2. Система отправляет ее в качестве входных данных на веб-сервер.

3. Сервер аутентификации генерирует один временной код и отправляет его в мобильное приложение.

4. Пользователь использует этот код в течение времени сеанса, по истечении сеанса пользователь должен снова войти в систему.

5. После входа в систему пользователь получает доступ к требуемым ресурсам.

Алгоритм аутентификации пользователей для регистрации в облачной среде через мобильное приложение включает шаги:

1. Пользователь нажимает на кнопку регистрации на странице сайта.

2. Идет запрос к веб-серверу на регистрацию.

3. Веб-сервер формирует страницу регистрации и возвращает ее пользователю.

4. Пользователь вводит информацию для регистрации.

5. Информация о пользователе передается на веб-сервер.

6. Веб-сервер проверяет информацию на правильность заполнения, если неверно, то формирует ошибки заполнения.

7. Веб-сервер возвращает ошибки заполнения пользователю.

8. Пользователь вносит исправления и заново отправляет информацию веб-серверу.

9. Веб-сервер подтверждает корректность заполнения.

10. Веб-сервер сохраняет информацию.

11. Веб-сервер передает сообщение о проведенной регистрации на e-mail.

Рассмотрены три варианта алгоритмов аутентификации с использованием метода 2FA. Первый алгоритм – проверка использования 2FA, включает следующие шаги:

1. Пользователь вводит имя пользователя и пароль.

2. Проверяется имя пользователя и пароль в существующей базе данных.

3. Если проверка неуспешна, вход для пользователя повторяется.

4. Проверяется необходимость аутентификации 2FA, если она требуется, то переход ко второму алгоритму 2FA.

5. Если 2FA не требуется, то пользователю предлагается другая аутентификация.

6. Если 2FA требуется, переход ко второму алгоритму.

Алгоритм второй (2FA требуется, пользователь не имеет токена):

1. Пользователь вводит запрос на сервер мобильных одноразовых паролей (Mobile One Time Password – MOTP).

2. Определятся статус пользователя.

3. Если пользователь не существует в базе данных или он отключен в базе данных, система показывает ошибку.

4. Если пользователь уже имеет токен и существует в базе данных, переход к третьему алгоритму (2FA требуется, пользователь имеет токен). Если пользователь не существует и не имеет токена, подсказка пользователю о простой регистрации

на веб-сайте.

5. Пользователь вводит информацию для регистрации.

6. После регистрации информация о пользователях сохраняется в БД.

7. Проверка ошибок. Если нет ошибки, это означает, что новый токен пользователя находится в МОТР.

8. Если есть ошибка, сообщение пользователю, чтобы попробовать еще раз обратиться в службу поддержки.

9. Если нет ошибок, это означает, что новый пользователь вошел на сервер МОТР.

Алгоритм третий (2FA требуется, пользователь входит на веб файл сервер – WFS):

1. Запрос пользователя, чтобы получить одноразовый пароль для входа в WFS.

2. Анализ запроса пользователя.

3. Если пользователь получает ОТР, использовать его для входа в WFS.

4. Если пользователь получил уведомление об ошибке, сообщить в службу технической поддержки.

5. Определение результатов проверки.

6. Если проверка прошла успешно, пользовательский доступ к среде WFS.

7. Если проверка не удалась или пользователь заблокирован, сообщить в службу технической поддержки.

Четвертая глава содержит описание программной реализации для проверки и применения разработанных моделей и алгоритмов выбора и организации аутентификации для финансовой организации. Разработана программная система, реализующая алгоритм выбора метода аутентификации. Применены результаты ее работы по выбору варианта аутентификации в ИКИС для пользователей мобильных приложений в реальной системе защиты информации банка ЗАО «Н.Е.Б. Банк». На основании работы средства даны рекомендации для модификации системы аутентификации в КИС этого банка.

Выбранная программная реализация аутентификации основана на средствах спецификации промежуточного программного обеспечения доступа OWIN (Open Web Interface for.Net). Подсистема Катана в этой спецификации поддерживает интегрированный конвейер OWIN в ASP.NET, который может обеспечивать защиту приложений, размещенных на сервере IIS, включая ASP.NET MVC, Web API, веб-формы. Катана включает четыре уровня: приложение, промежуточное программное обеспечение, сервер и хост.

Проект аутентификации в ЗАО «Н.Е.Б. Банк» по умолчанию имеет всю необходимую инфраструктуру: модели, контроллеры, представления (рисунок 2). Если пользователь входит в узел References, то увидит ряд библиотек, которые и содержат необходимые для авторизации и аутентификации классы [15]. Это

библиотеки средства OWIN, которые добавляют функциональность в проект, а также три библиотеки компонента ASP.NET Identity.

Осуществив регистрацию, можно войти в систему и начать пользоваться встроенной системой аутентификации в приложении ASP.NET MVC 5.

В файле web.config имеется строка подключения по умолчанию, которая задает каталог базы данных для управления доступом. В папке App_Data, пользователь видит созданную базу данных (рисунок 2).

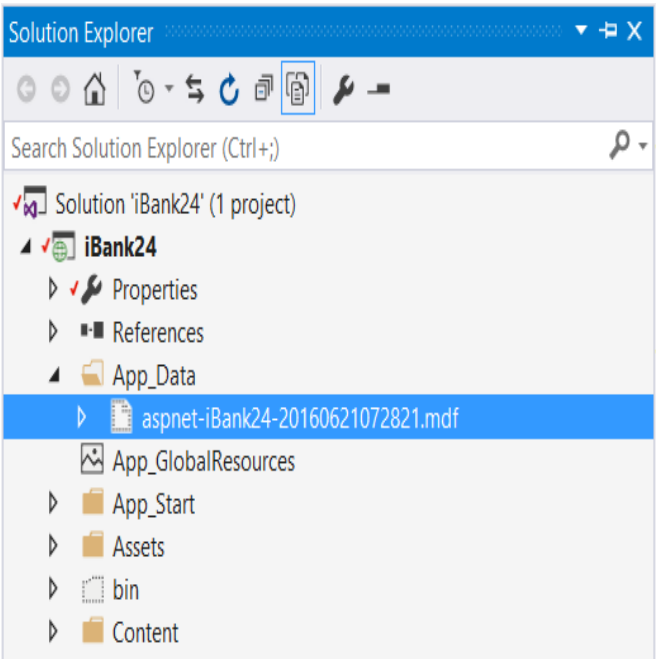

Рисунок 2. – Инфраструктура для аутентификации

После использования в системе безопасности ЗАО «Н.Е.Б. Банк» результатов, разработанных в диссертации (рекомендованной модели аутентификации от заключения программы АСА – использование технологии единого входа и двухфакторной аутентификации), проведены исследования безопасности по четырем показателям: поддержка безопасного протокола, мощность алгоритма шифрования, сопротивление атакам, цифровой сертификат. Интегрированная оценка ИБ (поддержка безопасного протокола, мощность алгоритма шифрования, сопротивление атакам, цифровой сертификат) до внедрения разработанных средств составляла 16,5 (18, 17, 14, 17) из 20 возможных. После внедрения разработанных средств эта оценка стала 18,25 (20, 18, 15, 20, рисунок 3).

Таким образом, интегрированная оценка ИБ для пользователей при работе с мобильными приложениями повысилась на 10,5 %, что говорит о технической эффективности методики, алгоритма и разработанного программного средства для параметрического выбора модели аутентификации в «Н.Е.Б. Банк». Показано

также, что с использованием дополнительной стоки входа хеш-функции для усиления пароля резко увеличивается время взлома.

Разработанные модели и средства аутентификации пользователей мобильных приложений использованы в учебном процессе, при выполнении НИР, а также при организации системы защиты для финансового учреждения.

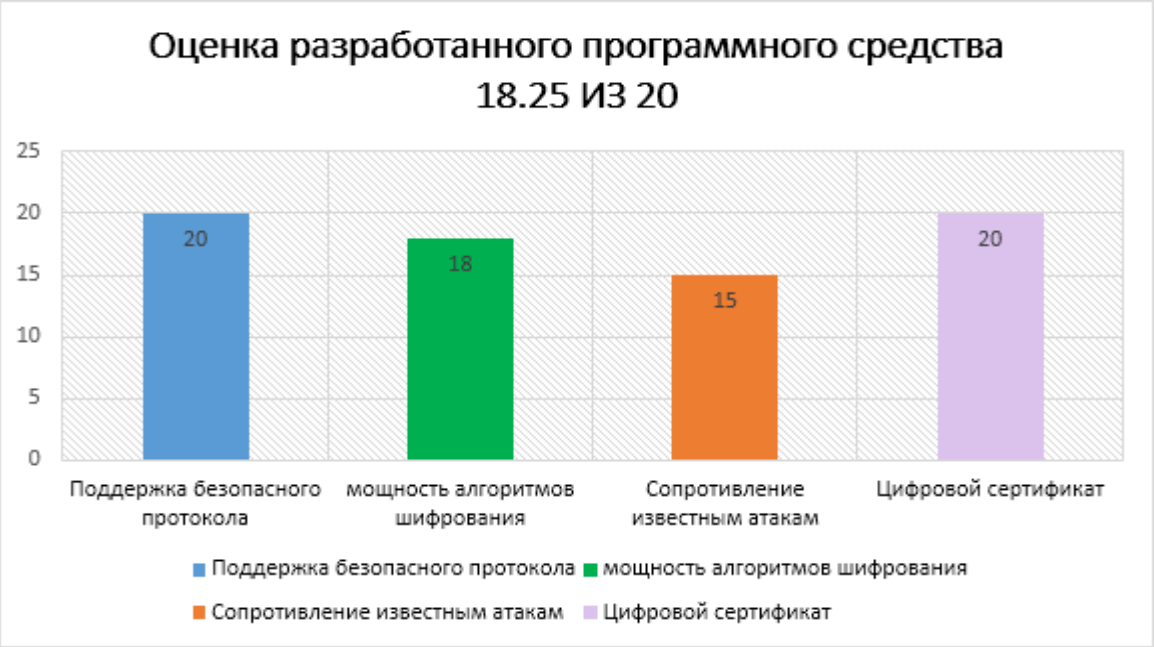

Рисунок 3. - Оценка технической эффективности модифицированного программного средства информационной защиты для ЗАО «Н.Е.Б. Банк»

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложена концепция ИКИС, базирующаяся на использовании в составе классической КИС предприятия технологий облачных вычислений, что дает модифицируемость средств аутентификации пользователей в зависимости от ситуации [1, 3, 6, 7, 9, 10]. Приведены символьные описания моделей аутентификации для работы пользователей КИС финансовой организации, которые можно хранить в базе знаний, модифицировать и использовать для автоматизированной поддержки принятия решений [2, 10, 11].

2. Разработаны символьные модели аутентификации пользователей мобильных приложений финансовых организаций: по паролю с сервером приложений, сертификатам, одноразовым паролям, ключам доступа, токенам, которые можно хранить в базе знаний, модифицировать и использовать для автоматизированной поддержки принятия решений по выбору лучшей модели аутентификации [2, 3, 4, 13].

3. Предложена методика выбора варианта аутентификации пользователей мобильных приложений на основе базы знаний моделей для ИКИС (с облачными вычислениями) финансовых учреждений, которая в отличие от известных решений поддерживает параметрический выбор модели аутентификации и создает основу для автоматизации выбора модели в зависимости от конкретной ситуации информационной безопасности для пользователей мобильных приложений [4, 8, 17, 18].

4. Разработаны алгоритм автоматизированного параметрического выбора аутентификации и алгоритмы трех видов аутентификации рекомендованного метода 2FA [5, 8, 12, 16]. Разработан и опробован программный вариант реализации параметрического выбора модели аутентификации для конкретной ситуации безопасности, который опробован при доступе к мобильным приложениям финансовой организации. Оценена эффективность разработанного программного средства [5, 8, 14, 15].

5. Разработанные модели, методика и алгоритмы реализованы в корпоративной сети финансовой организации ЗАО «Н.Е.Б. Банк». Представлена структура программной системы аутентификации для работы пользователей с мобильными приложениями. Проведены исследования последствий применения алгоритма и программы выбора лучшего вида аутентификации пользователей мобильных приложений в облачной среде, результаты которых показали повышение технической эффективности при работе в корпоративной сети финансовой организации на 10,5 % [5, 18].

Рекомендации по практическому использованию результатов

Исследованный в диссертации материал и сделанные на его основе выводы и предложения могут быть использованы:

1) на финансовых предприятиях для оптимизации доступа к мобильным приложениям в рамках программы импортозамещения;

2) в научных исследованиях – для развития положений принятия решений по аутентификации в интегрированных корпоративных информационных системах;

3) в учебном процессе – для учебных дисциплин «Основы защиты информации», «Методы защиты информации в инфокоммуникациях», «Теория системного анализа и принятия решений в инфокоммуникациях» в вузах Республики Беларусь.

Разработанные модели и средства выбора и организации аутентификации пользователей мобильных приложений использованы в корпоративной сети банка ЗАО «Н.Е.Б. Банк», учебном процессе Минского инновационного университета (МИУ), при выполнении НИР в лаборатории «Информационного управления» МИУ.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в рецензируемых научных журналах

1. Вишняков, В. А. Анализ и концепция развития информационной безопасности КИС и облачной платформы на базе интеллектуальных технологий / В. А. Вишняков, С. М. Гондаг, М. Г. Моздурани // Системный анализ и прикладная информатика. – 2014. – № 1-3. С. 55−59.

2. Вишняков, В. А. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях / В. А. Вишняков, М. М. Гондаг // Доклады БГУИР. – 2016. № 3 (97). – С. 111−114.

3. Вишняков, В. А. Концепция обеспечения безопасности корпоративных информационных систем с использованием облачных вычислений / В. А. Вишняков, М. М. Гондаг Саз, М. Г. Моздурани Шираз // Доклады БГУИР. – 2016. − № 8 (102). − С. 101−105.

4. Вишняков, В. А. Модели аутентификации в облачных вычислениях для мобильных приложений с интеллектуальной поддержкой выбора / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР. − 2017. − № 1 (103). – С. 82−86.

5. Вишняков, В. А. Алгоритм и реализация интеллектуального выбора модели доступа пользователей мобильных приложений в инфокоммуникациях / В. А. Вишняков, М. М. Гондаг Саз // Проблемы инфокоммуникаций. – 2019. − № 2. – С. 59−65.

Статьи в сборниках материалов научных конференций

6. Вишняков, В. А. Концепция инструментальной платформы информационной безопасности в среде облачных вычислений с использованием интеллектуальных технологий / В. А. Вишняков, М. М. Гондаг Саз, М. Г. Моздурани Шираз // Открытые семантические технологии проектирования интеллектуальных систем: материалы междунар. науч.-техн. конф., Минск, 19 – 21 февр. 2015 г. / Бел. гос. ун-т инфор. и радиоэлектр. редкол.: В. В. Голенков (отв. ред.) [и др.]. – Минск, 2017. – С. 173−176.

7. Vishniakou, U. A. Elements of information security in integration corporate information system on base of intelligence technologies use / U. A. Vishniakou, M. M. Ghondagh Sas, M. G. Mosdurany Shiras // Открытые семантические технологии проектирования интеллектуальных систем = Open Semantic Technologies for Intelligent Systems: материалы Междунар. науч.-техн. конф., Минск, 16 – 18 февр. 2017 г. / Бел. гос. ун-т инфор. и радиоэлектр. редкол. : В. В. Голенков (отв. ред.) [и др.]. – Минск, 2017. – С. 377 – 380.

8. Вишняков, В. А. Интеллектуальное управление выбором для доступа пользователей к мобильным приложениям / В. А. Вишняков, М. М. Гондаг Саз // Телекоммуникации : сети и технологии, алгебраическое кодирование и безопасность данных = Telecommunications : Networks and Technologies, Algebraic Coding and Data Security : материалы междунар. науч.-техн. семинара (Республика Беларусь, Минск, ноябрь – декабрь 2019 г.). – Минск : БГУИР, 2019. – С. 49–52.

Тезисы докладов на научных конференциях

9. Вишняков, В. А. Обзор и анализ безопасности работы пользователей в среде облачных вычислений / В. А. Вишняков, С. М. Гондаг // Технические средства защиты информации : тез. докладов XIII Белорусско-российской науч.-техн. конф., Минск, 4 - 5 мая 2015 г. ; редкол. : Л. М. Лыньков [и др.]. – Минск, 2015. – С. 29.

10. Гондаг, С. М. Состав безопасной работы пользователей в среде облачных вычислений / С. М. Гондаг, В. А. Вишняков // Технические средства защиты информации : тез. докладов XIII Белорусско-российской науч.-техн. конф., Минск, 4–5 мая 2015 г. ; редкол. : Л. М. Лыньков [и др.]. – Минск, 2015. – С. 29.

11. Вишняков, В. А. Анализ безопасной работы пользователей в корпоративных системах управления и облачных средах / В. А. Вишняков, С. М. Гондаг, М. Г. Моздурани // Современные средства связи : материалы 20-й междунар. науч. конф., Минск, 15 окт. 2015 г. / Выш. гос. колл. связи; редкол. : А. О. Зеневич [и др.]. – Минск: РИВШ, 2015. – С. 145-146.

12. Гондаг, Саз М. М. Алгоритмы аутентификации санкционированных пользователей в мобильной среде / С. М. Гондаг, В. А. Вишняков // Технические средства защиты информации : тез. докладов XIV Белорусско-российской науч.-техн. конф., Минск, 25–26 мая 2016 г. редкол. : Л. М. Лыньков [и др.]. – Минск, 2016. Минск : БГУИР, 2016. – С. 29.

13. Вишняков, В. А. Модель и программная поддержка работы пользователей в интегрированных корпоративных системах управления / В. А. Вишняков, С. М. Гондаг Саз, М. Г. Моздрурани Шираз / Современные средства связи : материалы XXI Междунар. науч.-техн. конф., 20–21 окт. 2016 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи , 2016. – С. 190-191.

14. Гондаг, Саз М. М. Компоненты системы аутентификации мобильных приложений в интегрированной КИС / М. М. Гондаг Саз, В. А. Вишняков // Технические средства защиты информации : тез. докл. XV Белорусско-российской науч.-техн. конф., Минск, 6 июня 2017 г. ; редкол. : Т. В. Борботько [и др.]. – Минск, 2017. – С. 47.

15. Гондаг, Саз М. М. Исследование и применение системы аутентификации мобильных приложений в интегрированной КИС / М. М. Гондаг Саз, В. А. Вишняков // Технические средства защиты информации: тез. докладов XVI Белорусско-российской науч.-техн. конф., Минск, 5 июня 2017 г., Минск : БГУИР, 2017. – С. 47.

16. Вишняков, В. А. Алгоритмы и методика аутентификации пользователей мобильных приложений в облачной среде / В. А. Вишняков, М. М. Гондаг Саз / Современные средства связи: материалы XXII Междунар. науч.-техн. конф., 19–20 окт. 2017 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи, 2017. – С. 333.

17. Вишняков, В. А. Аутентификации пользователей мобильных приложений в распределенной КИС / В. А. Вишняков, М. М. Гондаг Саз // Современные средства связи : материалы XXIII Междунар. науч.-техн. конф., 18 – 19 окт. 2018 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи, 2018. – С. 192.

18. Вишняков, В. А. Интеллектуальный выбор вида аутентификации пользователей мобильных приложений / В. А. Вишняков, М. М. Гондаг Саз // Современные средства связи : материалы XXIV Междунар. науч.-техн. конф., 19 – 20 окт. 2019 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск: Белорусская государственная академия связи, 2019. – С.158.

РЭЗЮМЭ

Гондаг Саз Мостафа Махамад

Мадэлі і алгарытмы аўтаматызаванага выбару і арганізацыі аўтэнтыфікацыі карыстальнікаў мабільных прыкладанняў фінансавых устаноў

Ключавыя словы: аўтэнтыфікацыя, прыняцце рашэнняў, мабільныя прыкладанні, мадэлі і алгарытмы, тэхналогіі, аўтаматызаваны выбар аўтэнтыфікацыі.

Мэта даследавання: распрацоўка базы мадэляў, алгарытмаў і праграмных сродкаў выбару і арганізацыі аўтэнтыфікацыі карыстальнікаў мабільных прыкладанняў у інтэграваных карпаратыўных інфармацыйных сістэмах (ІКІС) фінансавых прадпрыемстваў з аўтаматызацыяй параметрычнага выбару варыянту аўтэнтыфікацыі.

Метады даследавання і апаратура: тэорыя сетак, сістэмны аналіз, прыняцце рашэнняў, тэорыя аўтэнтыфікацыі, апрацоўка размеркаванай інфармацыі. Пры правядзенні даследаванняў выкарыстоўваліся мабільныя прылады і праграмы, воблачнае асяроддзе, база ведаў.

Атрыманыя вынікі і іх навізна: мадэлі знакавага апісання відаў аўтэнтыфікацыі карыстальнікаў мабільных прыкладанняў у ІКІС, на базе якіх фарміруецца база ведаў; методыка выбару варыянту мадэлі аўтэнтыфікацыі карыстальнікаў мабільных прыкладанняў на аснове базы ведаў мадэляў, якая падтрымлівае параметрычнае аўтаматызаванае прыняцце рашэнняў; распрацаваны алгарытм параметрычнага выбару мадэлі аўтэнтыфікацыі для карыстальнікаў мабільных прыкладанняў у ІКІС фінансавых устаноў і яго праграмная рэалізацыя; распрацаваны алгарытмы выбраных мадэляў аўтэнтыфікацыі для карыстальнікаў мабільных прыкладанняў у ІКІС фінансавых устаноў і іх праграмная рэалізацыя, што дазволіла атрымаць павышэнне інтэграванай ацэнкі інфармацыйнай абароны фінансавай арганізацыі.

Ступень выкарыстання: на прадпрыемствах ІТ для аптымізацыі доступу да мабільных прыкладанняў у карпаратыўных сетках з выкарыстаннем хмарных вылічэнняў; для выбару варыянтаў аўтэнтыфікацыі пры правядзенні даследаванняў у НІЛ Мінскага інаванцыйнага ўніверсітэта (МІЎ) і ў навучальным працэсе МІЎ.

Вобласць ужывання: выбар і арганізацыя аўтэнтыфікацыі ў карпаратыўных інфармацыйных сістэмах прадпрыемстваў з элементамі хмарных вылічэнняў пры працы з мабільнымі прыкладаннямі.

РЕЗЮМЕ

Гондаг Саз Мостафа Мохаммад

Модели и алгоритмы автоматизированного выбора и организации аутентификации пользователей мобильных приложений финансовых учреждений

Ключевые слова: аутентификация, принятие решений, мобильные приложения, модели и алгоритмы, автоматизированный выбор аутентификации.

Цель исследования: разработка базы моделей, алгоритмов и программных средств выбора и организации аутентификации пользователей мобильных приложений в интегрированных корпоративных информационных системах (ИКИС) финансовых предприятий с автоматизацией параметрического выбора варианта аутентификации.

Методы исследования и аппаратура: теория сетей, системный анализ, принятие решений, теория аутентификации, обработка распределенной информации. При проведении исследований использовались мобильные устройства и программы, облачная среда, база знаний.

Полученные результаты и их новизна: модели символьного описания видов аутентификации пользователей мобильных приложений в ИКИС, на базе которых формируется база знаний; методика выбора варианта модели аутентификации пользователей мобильных приложений на основе базы знаний моделей, которая поддерживает параметрическое автоматизированное принятие решений; разработан алгоритм параметрического выбора модели аутентификации для пользователей мобильных приложений в ИКИС финансовых учреждений и его программная реализация; разработаны алгоритмы выбранных моделей аутентификации для пользователей мобильных приложений в ИКИС финансовых учреждений и их программная реализация, что позволило получить повышение интегрированной оценки информационной защиты финансовой организации.

Степень использования: на ИТ-предприятиях для оптимизации доступа к мобильным приложениям в корпоративных сетях с использованием облачных вычислений; для выбора вариантов аутентификации при проведении исследований в НИЛ Минского инновационного университета (МИУ) и учебном процессе МИУ.

Область применения: выбор и организация аутентификации в корпоративных информационных системах предприятий с элементами облачных вычислений при работе с мобильными приложениями.

SUMMARY

Ghondagh Saz Mostafa Mohammad

Models and algorithms of automation selection and organization of user authentication for mobile applications of financical institutions

Keywords: authentication, decision making, mobile applications, models and algorithms, automated selection of authentication.

The aim of the work: development of models base, algorithms and software tools for selecting and organizing authentication of mobile application users in integrated corporate information systems (ICIS) of financial enterprises with the parametric selection of authentication model.

Research methods and equipment: network theory, system analysis, decision making, authentication theory, distributed information processing. During the research mobile devices and programs, cloud environment, knowledge base were used.

The obtained results and their novelty: model character descriptions of the types of user authentication mobile applications in ICIS to form the knowledge base; the method of selection of the variant of the model of user authentication, mobile-based applications, knowledge base models, which support parameter automatisazion decision-making; developed by algorithm of parametric model selection of authentication for users of mobile applications in the ICIS financial institutions and its implementation; algorithms of selected authentication models for mobile applications user in the integrated CIS of financial institutions and their software implementation were developed, which allowed to increase the integrated assessment of information security of a financial organization.

The degree of use: for small enterprises to optimize access to mobile applications on corporate networks with the use of cloud computing; for choice of options for to select authentication models in conducting research in the laboratory of Minsk Innovation University (MIU), in the educational process of MIU.

Field of application: information access control in corporate information systems businesses with elements of cloud computing for mobile applications.

Научное издание

Гондаг Саз Мостафа Мохаммад

МОДЕЛИ И АЛГОРИТМЫ АВТОМАТИЗИРОВАННОГО ВЫБОРА И ОРГАНИЗАЦИИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ФИНАНСОВЫХ УЧРЕЖДЕНИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.01 – Системный анализ, управление и обработка информации, 05.13.19 – Методы и системы защиты информации, информационная безопасность