Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.А. Прытков
31.03.2020 г.

Регистрационный № УД-6-1408/уч.

«ФИЛЬТРАЦИЯ ТРАФИКА В КОРПОРАТИВНЫХ СЕТЯХ»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:
1-98 80 01 «Информационная безопасность»

2020 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-98 80 01-2019 и учебных планов специальности 1-98 80 01 «Информационная безопасность».

Составитель:
Е.С. Белоусова, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук.

Рецензенты:
Кафедра телекоммуникационных систем учреждения образования «Белорусская государственная академия связи» (протокол № 8 от 25.02.2020г.);
В.Ю. Цветков, заведующий кафедрой инфокоммуникационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор.

Рассмотрена и рекомендована к утверждению:
Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 11 от 06.03.2020г.);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 7 от 20.03.2020г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа рассчитана на 198 учебных часов (6 з.е.)

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом УВО)				Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары	
1-98 80 01	Информационная безопасность	2	3	62	38	24	–	Экзамен

План учебной дисциплины в заочной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом УВО)				Контрольная работа	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары		
1-98 80 01	Информационная безопасность	2	3	16	8	8	–	1	Экзамен

Место учебной дисциплины.

Учебная дисциплина «Фильтрация трафика в корпоративных сетях» является неотъемлемой составной частью подготовки магистров по специальности 1-98 80 01 «Информационная безопасность» и относится числу дисциплин модуля «Безопасность веб-технологий».

Количество передаваемой информации с каждым днем увеличивается, что приводит к трудностям ее мониторинга и фильтрации, поэтому актуальным на сегодняшний день является владение навыками фильтрации данных, что успешно способствует блокированию нежелательного трафика. Учебная дисциплина «Фильтрация трафика в корпоративных сетях» тесно взаимосвязана со следующими дисциплинами: «Безопасность баз данных», «Организация данных в сетевых приложениях», «Виртуализация в информационных системах».

Цель преподавания учебной дисциплины: приобретение знаний по общим вопросам фильтрации трафика в компьютерных сетях, ознакомление с основ-

ными понятиями и терминологией в этой области, с проблемами противодействия сетевым атакам, а также формирование навыков по настройке оборудования для защиты компьютерных сетей.

Задачи учебной дисциплины:

– формирование базовых представлений о современных сетевых атаках и методах защиты от них;

– овладение различными методами противодействия компьютерным атакам, направленными на эффективное обеспечение информационной безопасности корпоративной сети;

– приобретение знаний о принципах и алгоритмах фильтрации данных;

– развитие навыков анализа и прогнозирования инцидентов информационной безопасности.

В результате изучения учебной дисциплины «Фильтрация трафика в корпоративных сетях» формируются следующие компетенции:

специализированные:

– применять средства анализа и фильтрации трафика в инфокоммуникационных сетях.

В результате изучения учебной дисциплины магистрант должен:

знать:

– основные определения и термины, касающиеся фильтрации данных;

– механизмы реализация компьютерных атак;

– методы фильтрации данных;

уметь:

– анализировать текущее состояние защищенности корпоративной сети;

– ставить задачу разработки оптимальной системы противодействия компьютерным атакам и составлять алгоритмы ее решения для конкретной корпоративной сети;

– определять цели и задачи, решаемые в рамках противодействия сетевым атакам;

– используя современные методы фильтрации данных, учитывать особенности функционирования конкретных систем обработки информации и оценивать их эффективность;

– практически решать задачи анализа и фильтрации данных;

владеть:

– современными методами анализа и фильтрации данных.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины.

№ п.п.	Название учебной дисциплины	Раздел, темы
1	Базируется на знаниях, полученных при освоении содержания образовательных программ по специальностям I ступени высшего образования	

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1	Способы классификации трафика	Модель OSI. Описание структуры данных на каждом из уровней модели OSI. Понятие трафика. Классификация трафика на основе портов. Классификация трафика в зависимости от источника.
2	Анализ сетевого трафика	Способы анализа сетевого трафика. Учёт состояния потока при анализе сетевого трафика. Градации полноты учёта состояния потока. Общая схема инфраструктурных алгоритмов анализа сетевого трафика.
3	Перехват сетевого трафика	Методы захвата пакетов. Снифферы. Конфигурация сетевой карты для сниффинга. Инструменты для захвата пакетов. Архитектура инструмента Wireshark. Структура NDIS (Network Driver Interface Specification).
4	Агрегирование пакетов в потоки	Методы агрегирования пакетов в потоки. Протоколы мониторинга потока данных. Обзор программ-анализаторов системного трафика. Протокол Cisco NetFlow. Настройка протокола NetFlow. Инструмент Tcpdump для анализа сетевого трафика.
5	Понятие фильтрации трафика	Понятие фильтрации данных. Классификация методов фильтрации данных. Архитектура системы фильтрации трафика. Определение зоны фильтрации данных.
6	Обнаружение сетевых атак	Атака подделки MAC адресов (MAC-спуфинг). Атака переполнения таблицы MAC адресов (ARP-спуфинг). Управление доступом с помощью фильтрации по MAC-адресам. Атака подмены IP-адреса (IP-спуфинг). Атака изменения адреса URL (URL-спуфинг, Link-спуфинг).
7	Технология VLAN	Использование технологии VLAN для ограничения передаваемого трафика между подсетями. Атака VLAN-hopping. Принципы создания и настройки защищенных VLAN. Примеры использования VLAN при планировании корпоративной сети.
8	Списки управления доступом	Списки управления доступом ACL: принципы функционирования, виды, основные рекомендации по настройке, конфигурирование на сетевых устройствах. Списки контроля доступа: стандартные, расширенные, возвратные, временные, динамические. Уменьшение угроз атак с помощью ACL.
9	Методы фильтрации в компьютерных сетях	MAC-фильтрация и IP-фильтрация. Методы фильтрации IP-пакетов и преобразование сетевых адресов. Анализ структуры web-страницы. Пакетные фильтры. Фильтр сеансового уровня. Фильтры прикладного уровня. URL-фильтрация и HTTP-фильтрация. Фильтрация веб-сайтов по URL-адресам и категориям. Виды URL-фильтрации. Настройка фильтрация HTTP-трафика. Принципы построения систем контентной фильтрации. Выполнение глубокого анализа сетевых протоколов (HTTP, HTTPS, FTP, FTPS и др.).
10	Программно-аппаратные методы фильтрации трафика	Виды межсетевых экранов. Пакетные фильтры. Межсетевые экраны с контролем соединений. Прокси-сервера. Межсетевые экраны нового поколения. Журналирование. Семейство межсетевых экранов CISCO ASA, Fortinet, ZBF, EcoFilter и др. Контроль доступа и сервисные политики на межсетевых экранах.
11	Организация защищенной корпо-	Основные элементы для защищенной корпоративной сети. Схема единой защиты корпоративной сети. Схема с защищаемой

№ тем	Наименование разделов, тем	Содержание тем
	ративной сети	закрытой и незащищаемой открытой подсетями. Схема с раздельной защитой закрытой и открытой подсетей на основе одного межсетевого экрана с тремя сетевыми интерфейсами
12	Топология сети при использовании межсетевых экранов	Принципы построения окружения межсетевого экрана. Несколько уровней межсетевых экранов. Конечные точки VPN. Планирование и внедрение межсетевого экрана. Конфигурирование, развертывание, управление.
13	Демилитаризованная зона	Методы организации демилитаризованной зоны (DMZ). Способы включения межсетевых экранов для создания демилитаризованной зоны. Конфигурация демилитаризованной зоны. Ограничение доступа к демилитаризованной зоне. Межсетевой экран с простой и DMZ-сетью.
14	Системы мониторинга	Мониторинг информационной безопасности. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS). Предотвращение утечек данных (DLP).
15	Аутентификация пользователей	Использование межсетевого экрана для централизованного управления доступом к ресурсам в сети. Аутентификация пользователей для доступа во внешнюю сеть
16	Система фильтрации интернет-трафика на основе методов машинного обучения	Классификация методов машинного обучения. Достоинства и недостатки. Применение методов машинного обучения для классификации IP-трафика. Архитектура системы фильтрации трафика. Используемые протоколы. Классификация трафика для метода машинного обучения. Библиотеки алгоритмов машинного обучения

2.Информационно-методический раздел

2.1 Литература

2.1.1 Основная

1. Информационная безопасность открытых систем : учебник. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников [и др.]. – М. : Горячая линия-Телеком, 2006. – 536 с.

2. Уилсон, Э. Мониторинг и анализ сетей. Методы выявления неисправностей / Э. Уилсон. - М. : ЛОРИ, 2013. – 350 с.

3. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие / В. В. Платонов. – М. : Академия, 2006. – 240 с. – (Высшее профессиональное образование).

2.1.2 Дополнительная

1. Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640-816 / У. Одом ; пер. с англ. – 3-е изд. – М. : Вильямс, 2013. – 752 с.

2. Вишняков В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели,

программно-аппаратные решения : монография / В. А. Вишняков. – Минск : Белорусская государственная академия связи, 2016. - 276 с.

3. Гафнер, В. В. Информационная безопасность : учебное пособие / В. В. Гафнер. – Ростов н/Д. : Феникс, 2010. – 324 с. – (Высшее образование).

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

1. Программный пакет моделирования и визуализации сети «Cisco Packet Tracer».
2. Межсетевой экран «Fortigate-60B».
3. Средство защиты электронной почты «FortiMail-100».
4. Система анализа сетевой активности «FortiAnalyzer-100B».
5. Межсетевой экран «Cisco ASA-5520».

2.3. Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков конфигурации сетевого оборудования для фильтрации трафика, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
2	Виды spoofing атак	Рассмотрение основных способов реализации атак MAC-spoofing, ARP-spoofing, IP-spoofing. Способов защиты от атак.	1
3	Уязвимости DHCP и DNS протоколов	Изучение способов перехвата трафика путем реализации атак, эксплуатирующих уязвимости DHCP и DNS протоколов.	1
4	Мониторинг трафика	Изучение мониторинга трафика в корпоративной сети на основе использования протокола NetFlow.	1, 5
7	Виртуальные локальные сети	Изучение принципов организации и настройки виртуальных локальных сетей для ограничения передачи трафика.	1
8	Настройка списков контроля доступа	Изучение типов списков контроля доступа и способов их конфигурации на сетевом оборудовании.	1, 2
9	Основы администрирования межсетевого экрана	Изучение организации консольного подключения к межсетевому крану. Овладение навыками использования базовых команд для базовой конфигурации межсетевого экрана.	2, 3, 5
10	Настройка межсетевого экрана с использованием веб-интерфейса	Изучение способов включения межсетевого экрана в корпоративную сеть. Овладение навыками конфигурации режимов работы межсетевого экрана NAT/Route и Transparent.	2, 3, 5

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
11	Настройка различных типов фильтрации	Изучение типов фильтрации и способов их конфигурации на межсетевом экране.	2, 3, 5
12	Настройка журналирования событий	Использование Dashboard для быстрого реагирования на инциденты. Настройка FortiAnalyzer для журналирования событий.	2, 3, 4
13	Организация сети с демилитаризованной зоной	Овладение навыками конфигурации демилитаризованной зоны на межсетевом экране.	1, 2, 5
14	Настройка DLP и IPS систем	Овладение навыками конфигурации DLP и IPS систем на межсетевом экране.	2, 3, 4
15	Ограничение доступа к ресурсам корпоративной сети	Изучение принципов конфигурации ограничения доступа пользователей к ресурсам корпоративной и глобальной сети.	2, 3, 5

2.4. Контрольная работа

Целью контрольной работы является углубление знаний, приобретение исследовательских навыков. Контрольная работа выполняется магистрантами заочной формы обучения на основе индивидуальных заданий. Вариант индивидуального задания контрольной работы выдается магистранту преподавателем.

№ темы по п.1	Наименование контрольной работы	Содержание	Обеспеченность по пункту 2.2
8	Моделирование защищенной корпоративной сети с использованием симулятора Cisco Packet Tracer	Разработка модели корпоративной сети с помощью оборудования анализа и фильтрации данных	1

2.5 Перечень рекомендуемых средств диагностики результатов учебной деятельности

Для диагностики результатов учебной деятельности могут использоваться следующие формы:

1. Защита лабораторной работы.
2. Устный опрос
3. Защита контрольной работы.
4. Коллоквиум

3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
1	Способы классификации трафика	2	-	-	9	Устный опрос
2	Анализ сетевого трафика	2	2	-	9	Устный опрос, защита лабораторной работы
3	Перехват сетевого трафика	2	2	-	8	Устный опрос, защита лабораторной работы
4	Агрегирование пакетов в потоки	2	2	-	8	Устный опрос, защита лабораторной работы
5	Понятие фильтрации трафика	2	-	-	9	Устный опрос
6	Обнаружение сетевых атак	4	-	-	8	Устный опрос
7	Технология VLAN	4	2	-	9	Устный опрос, защита лабораторной работы
8	Списки управления доступом	2	2	-	9	Устный опрос, защита лабораторной работы
9	Методы фильтрации в компьютерных сетях	2	2	-	8	Устный опрос, защита лабораторной работы
10	Программно-аппаратные методы фильтрации трафика	2	2	-	8	Устный опрос, защита лабораторной работы
11	Организация защищенной корпоративной сети	2	2	-	8	Устный опрос, защита лабораторной работы
12	Топология сети при использовании межсетевых экранов	2	2	-	9	Устный опрос, защита лабораторной работы
13	Демилитаризованная зона	2	2	-	9	Устный опрос, защита лабораторной работы
14	Системы мониторинга	2	2	-	9	Устный опрос, защита лабораторной работы
15	Аутентификация пользователей	2	2	-	8	Устный опрос, защита лабораторной работы
16	Система фильтрации интернет-трафика на основе методов машинного обучения	4	-	-	8	Устный опрос
	Текущая аттестация					**Экзамен**
	Итого	**38**	**24**	**-**	**136**	

3.2 Учебно-методическая карта учебной дисциплины в заочной форме обучения

Номер раз-дела, темы	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
1	Способы классификации трафика	1	-	-	11	Коллоквиум
2	Анализ сетевого трафика	1	-	-	11	Коллоквиум
3	Перехват сетевого трафика	1	2	-	9	Защита лабораторной работы
4	Агрегирование пакетов в потоки	-	-	-	12	Коллоквиум
5	Понятие фильтрации трафика	1	-	-	11	Коллоквиум
6	Обнаружение сетевых атак	-	-	-	12	Коллоквиум
7	Технология VLAN	-	-	-	14	Коллоквиум
8	Списки управления доступом	-	-	-	12	Коллоквиум, защита контрольной работы
9	Методы фильтрации в компьютерных сетях	2	2	-	8	Защита лабораторной работы
10	Программно-аппаратные методы фильтрации трафика	2	2	-	8	Защита лабораторной работы
11	Организация защищенной корпоративной сети	-	2	-	12	Защита лабораторной работы
12	Топология сети при использовании межсетевых экранов	-	-	-	12	Коллоквиум
13	Демилитаризованная зона	-	-	-	12	Коллоквиум
14	Системы мониторинга	-	-	-	12	Коллоквиум
15	Аутентификация пользователей	-	-	-	12	Коллоквиум
16	Система фильтрации интернет-трафика на основе методов машинного обучения	-	-	-	14	Коллоквиум
	Текущая аттестация					**Экзамен**
	Итого	**8**	**8**	**-**	**182**	

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Код и наименование специальности	Выпускающая кафедра	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего выпускающей кафедрой с указанием номера протокола и даты заседания кафедры
1	2	3	4
1-98 80 01 «Информационная безопасность»	Защиты информации	Нет	_____ Т.В. Борботько Протокол № 11 от 06.03.2020г.

Заведующий кафедрой защиты информации _____Т.В. Борботько