

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по науке
и международным связям

А.В. Толстиков

2 марта 2020 г.



СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ

Рабочая программа

для обучающихся по направлению подготовки

10.06.01 Информационная безопасность

Профиль (направленность):

Методы и системы защиты информации, информационная безопасность
форма обучения (очная)

Захаров А.А. Современные технологии защиты корпоративных сетей. Рабочая программа для обучающихся по направлению подготовки 10.06.01 Информационная безопасность, профиль (направленность): методы и системы защиты информации, информационная безопасность, форма обучения (очная). Тюмень, 2020.

Рабочая программа дисциплины (модуля) опубликована на сайте ТюмГУ: [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

1. Пояснительная записка

Целью дисциплины «Современные технологии защиты корпоративных сетей» является изучение основных типов атак, осуществляемых на сетевую инфраструктуру сети предприятия, а также - основных подходов, методов и средств по их предотвращению.

В **задачи** дисциплины «Современные технологии защиты корпоративных сетей» входит:

- изучение основных сервисов в защищенных корпоративных сетях;
- организация и настройка функциональных средств, предоставляемых различными вендорами сетевого оборудования;
- анализ современных протоколов и средств мониторинга в защищенных корпоративных сетях;
- изучение организационно-правовой базы обеспечения информационной безопасности корпоративных сетей.

1.1. Место дисциплины в структуре образовательной программы (ОП):

Данная дисциплина входит в блок ФТД Факультативы.

Для успешного усвоения данной дисциплины необходимо, чтобы аспирант владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Защита сетей», «Защита информационных систем персональных данных».

Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: - основные стандарты, используемые при передаче цифровой информации; - основные технологии передачи цифровой информации; - основные технологии защиты информации корпоративной сети. Умеет: - применять программные, аппаратные и программно-аппаратные средства защиты корпоративной сети.
ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования	Знает: - методы оценки эффективности средств защиты информации в корпоративной сети. Умеет: - применять существующий инструментарий для оценки защищенности корпоративной сети.
ПК-11 - способность к реализации мероприятий и механизмов формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	Знает: - организационно-правовые методы обеспечения информационной безопасности корпоративной сети. Умеет:

Таблица 1

Вид учебной работы		Всего часов (академические часы)	Часов в семестре (академические часы)
			3
Общий объем	зач. ед.	2	2
	час	72	72
Из них:			
Часы аудиторной работы (всего):		22	22
Лекции		14	14
Практические занятия		8	8
Часы внеаудиторной работы, включая самостоятельную работу обучающегося		50	50
Вид промежуточной аттестации (зачет, диф. зачет, кандидатский экзамен)			зачет

Текущий контроль не предполагает формализованной оценки работы обучающегося. В период проведения занятий по дисциплине преподаватель консультирует аспирантов по вопросам, возникающим у них в ходе самостоятельного изучения теоретического материала и выполнения контрольных работ. Проверка усвоения теоретического материала осуществляется во время проведения зачета.

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контак тной работы
			Лекции	Практические занятия	Лабораторные/ практические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Информационная безопасность корпоративной сети	24	4	4	0	0
2.	Программно-аппаратные средства защиты сети	26	6	4	0	0
3.	Организационно-правовые методы обеспечения безопасности корпоративной сети	20	4	0	0	0
4.	Зачет	2	0	0	0	2
	Итого (часов)	72	14	8	0	2

4.2. Содержание дисциплины (модуля) по темам

Тема 1. Информационная безопасность корпоративной сети

Определение и характеристика объектов защиты корпоративной сети. Модель угроз. Модель нарушителя. Стратегии защиты корпоративной сети. Средства защиты информации на сетевых устройствах уровня 2 и 3 модели OSI.

Тема 2. Программно-аппаратные средства защиты сети

Межсетевые экраны. Системы обнаружения и предотвращения вторжений. Антивирусы. Системы DLP.

Тема 3. Организационно-правовые методы обеспечения безопасности корпоративной сети

Аудит. Расследование инцидентов. Политика безопасности.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Информационная безопасность корпоративной сети	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.
2.	Программно-аппаратные средства защиты сети	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.
3.	Организационно-правовые методы обеспечения безопасности корпоративной сети	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Вопросы к зачету:

1. Модель угроз и модель нарушителя применимо к корпоративным сетям.
2. Угрозы и уязвимости канального уровня. Способы защиты канального уровня. Технология VLAN.
3. Угрозы и уязвимости сетевого уровня. Способы защиты сетевого уровня.
4. Технология VPN. Определение, принцип работы на примере конкретного протокола.
5. ACL. Межсетевые экраны. Суть подхода разбиения сети на зоны безопасности.
6. Системы обнаружения и предотвращения вторжений. Механизм работы.
7. Антивирусы. Классификация. Основные методы работы.
8. DLP-система. Предназначение. Примеры.
9. Аудит корпоративной сети. Стратегия аудита. Основные инструменты и методы аудита.
10. Расследование инцидентов информационной безопасности в корпоративной сети. Группа реагирования на инциденты информационной безопасности.

6.2. Критерии оценивания компетенций

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: - основные стандарты, используемые при передаче цифровой информации; - основные технологии передачи цифровой информации; - основные технологии защиты информации корпоративной сети. Умеет: - применять программные, аппаратные и программно-аппаратные средства защиты корпоративной сети.	опрос на занятии, зачет	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям, п. 4.29 «Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования	Знает: - методы оценки эффективности средств защиты информации в корпоративной сети. Умеет: - применять существующий инструментарий для оценки защищенности корпоративной сети.	опрос на занятии, зачет	

3.	ПК-11 - способность к реализации мероприятий и механизмов формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.	Знает: - организационно-правовые методы обеспечения информационной безопасности корпоративной сети. Умеет: - применять организационно-правовые методы для обеспечения информационной безопасности корпоративной сети.	опрос на занятии, зачет	
----	--	---	-------------------------	--

7. Учебно-методическое и информационное обеспечение дисциплины (модуля).

7.1. Основная литература:

1. Криптография и безопасность цифровых систем: Учебное пособие / Грибунин В.Г., Мартынов А.П., Николаев Д.Б. - Саратов:ФГУП"РФЯЦ-ВНИИЭФ", . - 411 с.: ISBN. - Текст : электронный. - URL: <https://znanium.com/catalog/product/950489> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

2. Петренко, С. А. Политики безопасности компании при работе в Интернет / Петренко С.А., Курбатов В.А., - 3-е изд., (эл.) - Москва :ДМК Пресс, 2018. - 397 с.: ISBN 978-5-93700-057-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/983161> (дата обращения: 01.03.2020). – Режим доступа: по подписке.

7.2. Дополнительная литература:

1. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100346> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

2. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100370> (дата обращения: 01.03.2020). — Режим доступа: для авториз. пользователей.

7.3. Интернет-ресурсы

1. Интернет ресурсы Academy Cisco <http://netacad.com>

7.4. Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) <https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true>

- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) <https://icdlib.nspu.ru/>

- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА <https://rusneb.ru/>

- Справочная правовая система КонсультантПлюс <http://www.consultant.ru/>

Наименование ПО

- Microsoft Office 365
- "Microsoft Imagine Academy (ранее Dreamspark):MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project"

7.5. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- гипервизор Oracle Virtual Box 5.*
- платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

7.6. Источники Интернет:

1. ФСБ России [Электронный ресурс]. – Режим доступа: <http://fsb.ru> (дата обращения 01.02.2020);
2. ФСТЭК России [Электронный ресурс]. – Режим доступа: <http://fstec.ru> (дата обращения 01.02.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

- эмулятор сетей PacketTracer.версия 7.x;
- эмулятор сетей GNS3 2.*
- эмулятор сетей eNSP 1.3.*
- гипервизор Oracle Virtual Box 5.*
- платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

9. Технические средства и материально-техническое обеспечение дисциплины.

Компьютерный класс с выходом в интернет и стандартное лабораторное и периферийное оборудование классом не ниже чем в приведенной ниже конфигурации.

- 3 маршрутизатора Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;
- 3 коммутатора Cisco Catalyst 2960;
- Набор последовательных кабелей и витой пары;
- 2 беспроводных маршрутизатора Linksys (предпочтительно Linksys WRT150N; допустимо использование моделей WRT54G, WRT300N и WRT350N) или аналогичные устройства SOHO.

Для проведения лекционных и практических занятий необходим проектор с разрешением не менее 800х1200, подключенный к компьютеру с выходом в Интернет.