

Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.01.02.0 «ОСНОВЫ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ
ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ»**

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль программы «Информационные технологии (по элективным модулям*)»

Автор(ы): ст. преп. А.Г. Уймин
ст. преп. В.В. Мешков

Одобрена на заседании кафедры информационных систем и технологий. Протокол от «20» января 2022 г. №5.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ИПО РГППУ. Протокол от «26» января 2022 г. №6.

Екатеринбург
2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Основы создания и эксплуатации защищенных компьютерных систем»: формирование у студентов профессиональных знаний и умений, связанных с использованием методов защиты информации и способов организации информационной безопасности на предприятии. приобретения студентами актуальных знаний и умений, позволяющих проявить себя в будущей профессиональной деятельности, реализовать свой творческий потенциал путем использования существующего программного обеспечения, а так же поиска новых, более эффективных и функциональных средств защиты информации.

Задачи:

- овладение теорией и методологией защиты информации;
- приобретение знаний и умений по организационному обеспечению информационной безопасности;
- обретение основ инженерно-технической защиты информации и криптографических методов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы создания и эксплуатации защищенных компьютерных систем» относится к части, формируемой участниками образовательных отношений, учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Операционные системы.
2. Компьютерные коммуникации и сети.
3. Математический аппарат для построения компьютерных сетей.
4. Программные средства защиты информации.
5. Системное и прикладное программирование.
6. Управление сетевыми сервисами.

Перечень учебных дисциплин, для которых необходимы знания, умения и владения, формируемые данной учебной дисциплиной:

1. Конфигурирование и поддержка сетевой инфраструктуры.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ПКС-2.3 Способен вести техническую документацию, связанную с эксплуатацией систем защиты информации автоматизированных систем.



В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

З1. Методику создания защищенных компьютерных систем;

З2. Технологии эксплуатации защищенных компьютерных систем.

Уметь:

У1. Создавать защищенные компьютерные системы;

У2. Эксплуатировать защищенные компьютерные системы.

Владеть:

В1. Технологиями создания и эксплуатации защищенных компьютерных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 час.), семестр изучения – 7, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоёмкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	7 сем.
	Кол-во часов
Общая трудоёмкость дисциплины по учебному плану	144
Контактная работа, в том числе:	42
Лекции	8
Лабораторные работы	34
Самостоятельная работа студента	102
Промежуточная аттестация, в том числе:	
Экзамен	7 сем.

**Распределение трудоёмкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*



4.2 Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Фундаментальные принципы безопасной сети	7	34	2	-	8	24
2. Авторизация, аутентификация и учет доступа (AAA).	7	36	2	-	8	26
3. Реализация технологий предотвращения вторжения	7	36	2	-	8	26
4. Реализация технологий VPN	7	38	2	-	10	26

**Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

4.3 Содержание разделов (тем) дисциплин

Раздел 1. Фундаментальные принципы безопасной сети

Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.

Безопасность Сетевых устройств OSI

Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.

Раздел 2. Авторизация, аутентификация и учет доступа (AAA).

Свойства AAA. Локальная AAA аутентификация. Server-based AAA.

Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.

Раздел 3. Реализация технологий предотвращения вторжения

IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS.

Безопасность локальной сети.

Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN.



Раздел 4. Реализация технологий VPN

VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN

Управление безопасной сетью

Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.

Cisco ASA.

Введение в Адаптивное устройство безопасности ASA. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

3. Традиционные образовательные технологии, которые ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

4. Информационно-коммуникационные образовательные технологии, при которых организация образовательного процесса, основывается на применении специализированных программных сред и технических средств работы с информацией. Используются для поддержки самостоятельной работы обучающихся с использованием электронной информационно-образовательной среды (ЭИОС), телекоммуникационных технологий, педагогических программных средств и др.

5. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли



занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1 Основная литература

1. Абросимов Л. И. Базисные методы проектирования и анализа сетей ЭВМ: учебное пособие / Абросимов Л. И. — Санкт-Петербург : Лань, 2018. — 212 с. — Режим доступа: <http://e.lanbook.com/book/112694>.

2. Берлин А.Н. Высокоскоростные сети связи [Электронный ресурс] / А.Н. Берлин. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. — 451 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/89433.html>.— ЭБС «IPRbooks»

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства : учебное пособие. - Саратов : Профобразование, 2017. - 544 с. - Режим доступа: <http://www.iprbookshop.ru/63592>.

6.2 Дополнительная литература

1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты : монография. - Саратов : Профобразование, 2017. - 446 с. - Режим доступа: <http://www.iprbookshop.ru/63800>.

2. Шаньгин В. Ф. Информационная безопасность и защита информации : учебное пособие. - Саратов : Профобразование, 2017. - 702 с. - Режим доступа: <http://www.iprbookshop.ru/63594>.

6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:



1. Интернет-портал по информационной безопасности. Режим доступа: <https://infobezlikbez.ru/>
2. Научная электронная библиотека eLIBRARY. Режим доступа: <https://elibrary.ru/defaultx.asp>
3. Науки и техника. Электронная библиотека. Режим доступа: <http://n-t.ru>
4. Электронная библиотека технической литературы. Режим доступа: www.tehlit.ru

Программное обеспечение:

1. Программное обеспечение для информационной безопасности Snort.
2. Операционная система Windows.
3. Электронно-библиотечная система IPRbooks.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».
2. Информационная система «Таймлайн».
3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.
2. Учебная аудитория сетевых технологий "D-link" - компьютерный класс.
3. Компьютерный класс.
4. Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием.
5. Помещения для самостоятельной работы.

