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 «ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки	44.03.04 Профессиональное обучение (по отраслям)
Профиль программы	«Информационные технологии (по элективным модулям*)»
Автор(ы):	ст. преп. С.В. Ченушкина

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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
2FF4095D1500DC80EC115E89D694AD8C
Владелец: Суслова Ирина Александровна
Действителен: с 09.02.2022 до 01.02.2023

Екатеринбург
2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Программные средства защиты информации»: развитие творческих подходов при решении сложных научно- технических задач, связанных с обеспечением программно-аппаратной защиты информации.

Задачи:

- изучение основ построения подсистем защиты информации в информационно-коммуникационных системах различной архитектуры;
- освоение основных программных средств и технологий обеспечения безопасности;
- оценки защищенности и обеспечения информационной безопасности объектов информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Программные средства защиты информации» относится к части, формируемой участниками образовательных отношений, учебного плана.

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

1. Базы данных.
2. Компьютерные коммуникации и сети.
3. Архитектура ПК и периферийные устройства.
4. Операционные системы.

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

1. Цифровая безопасность.
2. Конфигурирование и поддержка сетевой инфраструктуры.
3. Российские и международные стандарты информационной безопасности.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ПКС-2.1 Способен проводить работы по установке и техническому обслуживанию средств защиты информации;
- ПКС-2.2 Способен обеспечить бесперебойную работу средств связи сетей электросвязи (СССЭ), а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа (НСД);

- УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

З1. Современные методы и средства программно-аппаратной защиты информации и основные подходы к созданию таких средств;

З2. Назначение и принципы действия систем идентификации и аутентификации объектов и субъектов информационно-коммуникационных систем и сетей; методы и средства защиты от удаленных атак через глобальные сети; методы и средства защиты от разрушающих программных воздействий.

Уметь:

У1. Определять источники угрозы информационной безопасности информационно-коммуникационных систем и сетей;

У2. Разрабатывать меры защиты от выявленных угроз информационной безопасности;

У3. Выбирать и устанавливать программные средства защиты информации;

У4. Оценивать эффективность и надежность защиты информационно-коммуникационных систем и сетей.

Владеть:

В1. Профессиональной терминологией;

В2. Навыками внедрение и эксплуатации современных средств программно-аппаратной защиты информации;

В3. Навыками разработки и использования межсетевых экранов и систем обнаружения и предотвращения вторжений.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 6 зач. ед. (216 час.), семестры изучения – 5, 6, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	5, 6 сем.
	Кол-во часов
Общая трудоемкость дисциплины по	216

учебному плану	
Контактная работа, в том числе:	76
Лекции	16
Лабораторные работы	60
Самостоятельная работа студента	140
Промежуточная аттестация, в том числе:	
Зачет	5 сем.
Экзамен	6 сем.
Курсовая работа	6 сем.

**Распределение трудоемкости 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. Организация информационной защиты системы	5	18	2	-	6	10
2. Управление доступом к данным	5	30	2	-	8	20
3. Методы защиты передачи данных	5, 6	37	2	-	10	25
4. Построение виртуальных частных сетей	6	30	2	-	8	20
5. Базовые средства защиты серверных операционных систем.	6	41	4	-	12	25
6. Развертывание и администрирование платформы "1С: Предприятие"	6	30	2	-	8	20
7. Дополнительные средства и технологии защиты.	6	30	2	-	8	20

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

4.3 Содержание разделов (тем) дисциплин

Раздел 1. Организация информационной защиты системы

Организация информационной защиты системы.

Раздел 2. Управление доступом к данным

Система доверительных отношений в информационных системах. Стандартные и специальные права доступа

Раздел 3. Методы защиты передачи данных

Межсетевые экраны уровня соединений. Прокси-сервера. Сетевые анализаторы.

Раздел 4. Построение виртуальных частных сетей

Удаленное администрирование. Построение единой сети предприятия.

Раздел 5. Базовые средства защиты серверных операционных систем.

Администрирование серверов на базе Windows и консольного типа.

Раздел 6. Развертывание и администрирование платформы "1С: Предприятие"

Настройка файлового, кластерного режима работы. Резервное копирование конфигураций. Настройка прав доступа.

Раздел 7. Дополнительные средства и технологии защиты.

Системы обнаружения вторжений. Технология "HoneyPot". Сканеры безопасности и др.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Для поддержки самостоятельной работы обучающихся использованы информационно-коммуникационные образовательные технологии, в частности, облачные технологии, электронная информационно-образовательная среда (ЭИОС), электронные средства обучения и электронно-библиотечные системы. При этом результативность организации самостоятельной работы обучающихся существенно повышается за счет доступности материалов, упорядоченности работ и возможности получения консультации преподавателя.

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

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. Кейс-технологии применяются как способ обучать решению практико-ориентированных неструктурированных образовательных научных или профессиональных проблем. Применяется как при чтении лекций, так и при проведении семинарских, практических и лабораторных занятий.

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. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 192 с. — Режим доступа: https://e.lanbook.com/book/63241. — Загл. с экрана.

2. Ботуз С. П. Интеллектуальные интерактивные системы и технологии управления удаленным доступом. Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet : учебное пособие. - Москва : Солон-пресс, 2016. - 340 с. - Режим доступа: http://www.iprbookshop.ru/26917.

3. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных

Технологий (ИНТУИТ), 2016. — 242 с. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html.— ЭБС «IPRbooks»

4. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 с. — 978-5-94774-708-9. — Режим доступа: http://www.iprbookshop.ru/62827.html.— ЭБС «IPRbooks»

5. Лапонина О.Р. Межсетевое экранирование [Электронный ресурс] : учебное пособие / О.Р. Лапонина. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 344 с. — 978-5-4487-0078-1. — Режим доступа: http://www.iprbookshop.ru/67391.html.— ЭБС «IPRbooks»

6.2 Дополнительная литература

1. Пушкарёв, В.В. Защита информационных процессов в компьютерных системах [Электронный ресурс] : учеб. пособие / В.В. Пушкарёв, В.П. Пушкарёв. — Электрон. дан. — Москва : ТУСУР, 2012. — 131 с. — Режим доступа: https://e.lanbook.com/book/4925. — Загл. с экрана.

2. Васильев, В.И. Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Машиностроение, 2013. — 172 с. — Режим доступа: https://e.lanbook.com/book/5792. — Загл. с экрана.

6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:

1. ITSec.Ru - портал для профессионалов информационной безопасности. Режим доступа: http://www.itsec.ru/

2. Интернет-портал по информационной безопасности. Режим доступа: https://infobezlikbez.ru/

Программное обеспечение:

1. Операционная система Windows.
2. Операционная система Ubuntu.
3. Программное обеспечение виртуализации DOSBox.
4. Среда разработки 1С: Предприятие.
5. Офисная система Office Professional Plus.

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. Компьютерный класс.
2. Учебная аудитория для проведения занятий лекционного типа.
3. Помещения для самостоятельной работы.
4. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.