Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1156874	Защита информации

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информационная безопасность телекоммуникационных систем	**Код ОП** 1. 10.05.02/22.01
Направление подготовки 1. Информационная безопасность телекоммуникационных систем	**Код направления и уровня подготовки** 1. 10.05.02

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
2	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защита информации

1.1. Аннотация содержания модуля

Модуль «Защита информации» посвящен изучению существующих программно аппаратных средств защиты компьютерной информации и автоматизированных систем в защищенном исполнении. Изучаются основные направлений защита информации, защита информации, обрабатываемой в распространенных клиентских приложениях, защита компьютерной информации от вредоносных программ, защита информации, хранимой на машинных носителях и специализированные программно аппаратные средства защиты.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Программно-аппаратные средства защиты информации	5
2	Защита информации в компьютерных сетях	6
3	Защита информации в системах беспроводной связи	4
4	Методы резервирования и восстановления информации	3
5	Комплексное обеспечение защиты информации в объектах информатизации	4
	ИТОГО по модулю:	22

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Основы информационной безопасности
Постреквизиты и кореквизиты модуля	1. Защита информации в информационно-управляющих систем

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)

1	2	3
Защита информации в компьютерных сетях	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Работать с различными источниками информации У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей	З-1 - Трактовать отечественные и зарубежные стандарты в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов З-2 - Понимать и излагать правила создания технического задания на создание подсистем безопасности информационных систем З-3 - Перечислять основные угрозы безопасности информации и модели нарушителя в информационных системах У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

		У-2 - Разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации П-1 - Разрабатывать политики безопасности различных уровней П-2 - Оценивать риски в области информационной безопасности П-3 - Разрабатывать проекты нормативных материалов, регламентирующих работу по комплексной защите информации
Защита информации в системах беспроводной связи	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Работать с различными источниками информации У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости	З-1 - Трактовать отечественные и зарубежные стандарты в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов З-2 - Понимать и излагать правила создания технического задания на создание

	телекоммуникационных систем и сетей	подсистем безопасности информационных систем З-3 - Перечислять основные угрозы безопасности информации и модели нарушителя в информационных системах У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности У-2 - Разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации П-1 - Разрабатывать политики безопасности различных уровней П-2 - Оценивать риски в области информационной безопасности П-3 - Разрабатывать проекты нормативных материалов, регламентирующих работу по комплексной защите информации
Комплексное обеспечение защиты информации в объектах информатизации	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Работать с различными источниками информации У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества,

		основными подходами к противодействию угрозам информационной безопасности
	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей	З-1 - Трактовать отечественные и зарубежные стандарты в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов З-2 - Понимать и излагать правила создания технического задания на создание подсистем безопасности информационных систем З-3 - Перечислять основные угрозы безопасности информации и модели нарушителя в информационных системах У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности У-2 - Разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации П-1 - Разрабатывать политики безопасности различных уровней П-2 - Оценивать риски в области информационной безопасности П-3 - Разрабатывать проекты нормативных материалов, регламентирующих работу по комплексной защите информации
Методы резервирования и восстановления информации	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Работать с различными источниками информации

		У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
Программно-аппаратные средства защиты информации	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности У-1 - Работать с различными источниками информации У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности
	ОПК-20 - Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	З-1 - Определять и объяснять существующие виды уязвимостей У-1 - Обосновывать методику выявления уязвимостей в защищенных сетевых ресурсах П-1 - Оформлять отчеты по выявленным уязвимостям

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
2	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ
3	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
PI	Принципы Фон-Неймана и общее устройство современного компьютера.	Общее устройство и логика работы современного компьютера. Устройство управления и арифметикологическое устройство. Адреса и адресация. Линейность и однородность памяти. Двоичное кодирование. Программное управление. Регистры процессора. Счетчик команд. Программная и аппаратная организация стека. Передача управления. Регистр флагов. Режимы работы процессоров. Организация памяти в незащищенном режиме. Параграфы и сегменты. Адресация в незащищенном и защищенном режимах. Таблицы дескрипторов. Техника Родена. Начальная загрузка. BIOS. POST. Область данных BIOS. LBA. MBR. Загрузочный сектор. Блок управления памятью. Запуск и исполнение программ. Линия A20. HMA. UMA. EMM. EMS. Режим SMM. Гарвардская и принстонская архитектуры
PII	Работа с внешними устройствами	Системная шина. Внешнее устройство. Контроллер устройства. Регистры и области данных устройства. Общая схема подключения внешних устройств. Пространство ввода-вывода. Порт ввода-вывода. Отображение регистров и областей данных

		в оперативную память и пространство ввода-вывода. Порты-алиасы.
PIII	Механизм прерываний	Поллинг и прерывания – логика работы. Классификация прерываний. Аппаратные, программные, внешние, внутренние, маскируемые, немаскируемые, пошаговые, отладочные прерывания. Исключения и особенности их обработки. NMI и SMI. Обработчик прерывания. Контекст. Вектор прерывания. Таблица векторов прерываний. Последовательность обработчиков и правила работы обработчиков в последовательности. Резидентная программа. Мультиплексное прерывание.
PIV	Контроллер прерываний	Общая схема подключения, алгоритм и режимы работы контроллера прерываний. Подключение внешних устройств к контроллеру. Регистр запросов, регистр состояния и регистр масок. Назначение векторов прерываний устройствам. Запросы на прерывание уровнем и фронтом. Алгоритм вызова обработчика с учетом механизма приоритетов. Подключение нескольких устройств к одному уровню прерываний. Совместная работа обработчиков на одном уровне. Отбой контроллера и отбой устройства. Работа нескольких контроллеров в каскаде с примерами
PV	Организация ввода-вывода	Видеопамять и видеорежимы. Структура видеопамяти. Алфавит и кодировка. Знакоместо и его адрес в памяти. Код и атрибут символа. Отображение информации в текстовых и графических режимах. Видеостраницы. Устройство клавиатуры. Скан-код символа. Работа клавиатурных драйверов. Устройство кольцевого буфера и правила работы с ним. Работа с манипулятором «мышь».
PVI	Таймеры, измерение времени и генерация звука	Системный таймер и режимы его работы. Отличие генератора частоты от генератора меандра. Схема подключения системного таймера. Алгоритм программирования и регистры каналов. Работа системного таймера с контроллером прерываний и контроллером памяти. Алгоритм генерации звука. Программируемый периферийный интерфейс. Работа с часами реального времени и CMOS. Измерение временных промежутков с использованием возможностей таймеров.
PVII	Компьютерная память	Статическая, динамическая, синхронная и асинхронная память. Регенерация памяти. Алгоритмы чтения и записи. Латентность, время доступа и время деактивации. DRAM. SDRAM. FPM. EDO. BEDO. DDR. DDR2. DDR3. SRAM. SSRAM. Энергонезависимая память. ROM. PROM. EPROM. EEPROM. FRAM. Shadow ROM. Механизмы регенерации. CBR. FLASH-память. Работа полевого транзистора с плавающим затвором. Понятие кадра. NOR. NAND. Работа микросхем SLC, MLC и X3.
PVIII	Прямой доступ к памяти	Механизм прямого доступа к памяти (DMA). Устройство и алгоритм работы контроллера DMA. Режимы работы и

		программирование. Схема подключения контроллера. Примеры работы устройств с использованием контроллера.
PIX	Системные шины. ISA, EISA, PCI	Системные шины и их характеристики. Пропускная способность. Протокол шины. Шина ISA. Шина адреса. Шина данных. Шина управления. BUSmastering. Распределение ресурсов. Спецификация протокола ISA PnP. Протокол изоляции. Шина EISA. Архитектура шины PCI. Адресация устройств на шине. Обработка прерываний в системе с шиной PCI. Конфигурационное пространство PCI. Мезонинная шина. Эмуляция ISA и PCI в современных чипсетах.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-20 - Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	З-1 - Определять и объяснять существующие виды уязвимостей

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Электронные ресурсы (издания)

1. Магда, Ю. С.; Программирование и отладка C/C++ приложений для микроконтроллеров ARM : практическое пособие.; ДМК Пресс, Москва; 2012; https://biblioclub.ru/index.php?page=book&id=245894 (Электронное издание)

Печатные издания

1. Гук, Гук М.; Аппаратные интерфейсы ПК : Наиболее полн. и подроб. рук..; Питер, Москва; СПб.; Н. Новгород и др.; 2002 (2 экз.)

2. Колесниченко, О. В., Шишигин, И. В.; Аппаратные средства PC : энцикл. аппаратных ресурсов персонального компьютера : наиб. полн. рук..; БХВ-Петербург, Санкт-Петербург; 2003 (30 экз.)

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

http://lib.urfu.ru/mod/data/view.php?id=1379]

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

5	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
6	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации в компьютерных сетях

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Золотых Максим Олегович	кандидат технических наук, без ученого звания	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Золотых Максим Олегович, Доцент,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.
2	Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования

		руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows 2000-XP. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого
3	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
4	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory
5	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и

		ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационнотелекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникацио	У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения

			нных систем и сетей	информационной безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в компьютерных сетях

Электронные ресурсы (издания)

1. , Синадский, , Н. И.; Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие.; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2014; http://www.iprbookshop.ru/65983.html (Электронное издание)

Печатные издания

1. , Андрончик, А. Н., Богданов, В. В., Домуховский, Н. А., Коллеров, А. С., Синадский, Н. И., Хорьков, Д. А., Щербаков, М. Ю.; Защита информации в компьютерных сетях. Практический курс : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем".; УГТУ-УПИ, Екатеринбург; 2008 (1 экз.)

2. Хорев, П. Б.; Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника".; Academia, Москва; 2005 (29 экз.)

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

http://lib.urfu.ru/mod/data/view.php?id=1379]

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в компьютерных сетях

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

6	Курсовая работа/ курсовой проект	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации в системах беспроводной связи

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Дудоров Евгений Николаевич	кандидат технических наук, доцент	Доцент	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Дудоров Евгений Николаевич, Доцент,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Основы построения беспроводных сетей	Беспроводные сети передачи информации. История и основные понятия. Краткий экскурс в историю беспроводной связи. Основные термины и понятия. Стандарт IEEE 802.11.Сетевая архитектура. Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Основы организации и функционирования сетей. Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиентсервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети.
2	Технологии обеспечения безопасности в беспроводных сетях	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность. Защита топологии сети. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование. Виртуальные частные сети. Защита сетевого трафика и

		компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами. Средства повышения надежности функционирования Сетей. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях
3	Проектирование защищенных беспроводных сетей	Политика безопасности Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности. Критерии оценки безопасности сетевых ОС Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения. Анализ угроз, уязвимостей и атак. 6 Классификация беспроводных систем, анализ состава и архитектурных особенностей построения БС, изучение функциональных особенностей современных стандартов БС, проектирование системы информационной безопасности БС на основе моделирования ключевых процессов при помощи аппарата анализа рисков.
4	Методы и алгоритмы прогнозирования эффективности защиты БС	Анализ угроз, уязвимостей и атак. Классификация беспроводных систем, анализ состава и архитектурных особенностей построения БС, изучение функциональных особенностей современных стандартов БС, проектирование системы информационной безопасности БС на основе моделирования ключевых процессов при помощи аппарата анализа рисков. Анализ возможных сценариев атак. Постановка задачи оценки эффективности наборов средств защиты беспроводных сетей. Рисканализ беспроводных сетей Разработка рискшанс модели компонентов беспроводных сетей группы стандартов IEEE 802.11.Анализ эффективности. Оценка эффективности системы обеспечения безопасности беспроводных сетей группы стандартов IEEE 802.11.Механизмы управления Организация и управление экспертной системой для оценки основных показателей защищенности беспроводной сети Оптимизация выбора мер и средств защиты Методический подход к оптимизации выбора мер и средств защиты беспроводных сетей группы стандартов IEEE 802.11

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей	У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

Электронные ресурсы (издания)

1. Ермаков, , Д. Г.; Применение антивирусных программ для обеспечения информационной безопасности; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2013; http://www.iprbookshop.ru/66577.html (Электронное издание)

Печатные издания

1. Проскурин, В. Г.; Защита программ и данных : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 090900 "Информ. безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информ. безопасность автоматизир. систем".; Академия, Москва; 2011 (25 экз.)

2. Платонов, В. В.; Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105.; Академия, Москва; 2006 (10 экз.)

3. Степанов, Е. А., Корнеев, И. К.; Информационная безопасность и защита информации : Учеб. для студентов вузов, обучающихся по спец. "Документоведение и документационное обеспечение управления".; ИНФРА-М, Москва; 2001 (5 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Faculty EES

5	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы резервирования и восстановления информации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Князева Наталия Сергеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
3	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Князева Наталия Сергеевна, Старший преподаватель,**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Технологии хранения данных	Технология хранения данных. Логика хранения данных. Причины потерь информации. Виды потерь информации. Защита и безопасность данных
Р2	Стратегия защиты и восстановления данных	Обеспечение бесперебойного электропитания. Виды защитных устройств. Источники бесперебойного питания. Виды защитного программного обеспечения. Программы контроля целостности данных. Антивирусные программы. Программные средства разграничения и контроля доступа. Средства идентификации пользователей. Средства контроля действий пользователя. Средства контроля процессов. Программные средства сетевой защиты. Системы обнаружения атак. Сетевые сканеры и антиспамеры. Средства криптографической защиты
Р3	Сохранение данных при резервном копировании	Типы резервного копирования. Резервное копирование файлов и образов. Резервное копирование по плану. Полное, дифференциальное и инкрементное резервное копирование. Резервное копирование с агентами и без них. Выбор решений для резервного копирования.

Р4	Безопасное хранение резервных копий	Настройка политики хранения данных. Выбор ПО, оборудования и сайтов. Сжатие и дедупликация данных. Оценка стоимости хранения.
Р5	Технологии резервного копирования данных	Архивация и резервное копирование. Методы резервного копирования. Средства резервного копирования. Устройства хранения данных. Технология RAID. Программы для резервного копирования. Программы архивации данных.
Р6	Управление резервным копированием	Возможности резервного копирования. Оптимальный план восстановления и проверка его эффективности. Отслеживание исполнения плана резервирования данных. Настройка окна резервного копирования.
Р7	Настройка системных параметров резервирования и восстановления информации	Установка параметров BIOS. Основные функции BIOS. Параметры загрузки системы. Установка параметров файловой системы. Организация хранения данных на жестком диске. Логическая структура жесткого диска. Хранение данных в файловой системе FAT32. Хранение данных в файловой системе NTFS. Конфигурирование логических дисков. Монтирование дисков. Инструменты для работы с разделами дисков. Копирование разделов. Создание резервного раздела. Конвертирование разделов. Обслуживание дисков. Дефрагментация диска. Средства дефрагментации Windows и сторонних производителей. Профилактика аппаратных сбоев и отказов. Настройка интерфейса файловой системы.
Р8	Восстановление системной информации	Восстановление BIOS. Коррекция параметров BIOS. Установка параметров BIOS по умолчанию. Перезапись BIOS. Устранение проблем с загрузкой системы, файлами управления загрузкой и драйверами устройств. Средства восстановления Windows. Меню режимов загрузки Windows. Восстановление системы и создание новой точки восстановления. Программа проверки и восстановления системных файлов. Восстановление системного реестра. Описание реестра Windows. Средства восстановления реестра Windows. Программы для работы с реестром от сторонних разработчиков
Р9	Восстановление данных пользователя системы	Общие правила восстановления данных. Выбор программных средств восстановления. Восстановление данных на жестком диске. Восстановление данных на сменных носителях.
Р10	Восстановление данных на жестких дисках	Восстановление логической структуры диска. Восстановление главной загрузочной записи. Восстановление удаленных и «потерянных» разделов. Восстановление данных в файловой системе NTFS. Восстановление элемента таблицы разделов. Восстановление загрузочного сектора раздела NTFS. Восстановление служебной информации в MFT

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Формирование информационной культуры в сети интернет	целенаправленная работа с информацией для использования в практических целях	Технология самостоятельной работы	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы резервирования и восстановления информации

Электронные ресурсы (издания)

1. Трофимов, В. Б.; Интеллектуальные автоматизированные системы управления технологическими объектами: учебно-практическое пособие : учебное пособие.; Инфра-Инженерия, Москва, Вологда; 2016; https://biblioclub.ru/index.php?page=book&id=444175 (Электронное издание)

Печатные издания

1. Бигелоу, Стивен Дж., С. Дж., Гороховский, Ю.; Сети: поиск неисправностей, поддержка и восстановление; БХВ-Петербург, Санкт-Петербург; 2005 (6 экз.)

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

http://lib.urfu.ru/mod/data/view.php?id=1379]

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы резервирования и восстановления информации

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Student EES

5	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Комплексное обеспечение защиты информации в объектах информатизации

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Старший преподаватель	
2	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ
3	Синадский Николай Игоревич	кандидат технических наук, доцент	Доцент	

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № _9_ от _20.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ**
- **Синадский Николай Игоревич, Доцент,**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Теоретические основы компьютерной безопасности	Основные понятие и предметная область информационной безопасности (ИБ), ее место в системе национальной безопасности Российской Федерации. Особенности информации как объекта защиты. Основные свойства и виды защищаемой информации. Источники и носители защищаемой информации. Роль человеческого фактора в информационной системе Классификация категорий пользователей и других лиц по их влиянию на безопасность компьютерной информации. Социально психологический портрет хакера. Анализ и классификация угроз ИБ, виды ущерба от реализовавшихся угроз и его последствия. Основные направления информационной защиты. Силы, средства и методы и обеспечения информационной безопасности объектов. Политика информационной безопасности. Системы ограничения и разграничения доступа к защищаемым данным. Основные модели разграничения доступа. Политика разграничения доступа.
2	Криптографические методы защиты информации	Основные понятия криптографии: алгоритмы и ключи шифрования; простейшие шифры и их свойства: шифры простой замены, перестановки, гаммирования; теорема Шеннона; блоковые и потоковые шифры; современные стандарты шифрования; атаки на криптосистему;

		теоретическая и практическая криптостойкость шифров; имитостойкость и помехоустойчивость шифров. Принципы построения криптографических алгоритмов с открытыми ключами. Сравнительная характеристика систем симметричного и несимметричного шифрования. Алгоритмы DES и ГОСТ 28147-89; асимметричные криптосистемы с открытыми ключами; понятие необратимых и односторонних функций; схема открытого распределения ключей Диффи-Хеллмана; стандарты функций хэширования России и США. Электронная подпись (ЭП); способы организации ЭП; аутентификация сообщений и пользователей в современных системах информационных технологий на базе ЭП; применение хэш-функций в схемах ЭП. Стандарты ЭП России и США. Особенности аппаратной и программной реализации современных криптосистем. Средства шифрования, предоставляемые прикладными программами офисного пакета.
3	Программно-аппаратные средства обеспечения информационной безопасности	Методы и средства ограничения доступа к компонентам ЭВМ и входа в систему; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; контроль целостности программного обеспечения и аппаратуры; идентификация пользователей, программно-аппаратные методы аутентификации личности пользователей, парольные системы. Защита на вход в компьютерную систему средствами BIOS; настройки параметров безопасности и оптимизация ресурсов в CMOS-памяти. Защита информации на машинных носителях. Проблемы хранения данных, их содержание и причины возникновения. Логическая организация дискового пространства. Общие характеристики файловых систем с точки зрения информационной безопасности. Обеспечение защиты компьютерной информации на машинных носителях. Защищенные файловые системы. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Восстановление информации с резервных копий. Профилактика магнитных носителей и файловой системы ПЭВМ. Виды и стратегии резервирования компьютерной информации. Использование стандартных программ-архиваторов для резервирования информации. Отказоустойчивые дисковые конфигурации (RAID). Технология RAID, резервирование, кластеризация. Угрозы, связанные с возможными атаками с целью осуществления несанкционированного доступа. Организация защищенных компьютерных систем на базе ОС Windows XP. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа. Аудит локальной системы; настройка и просмотр аудита. Область действия настроек

		аудита. Средства мониторинга и оптимизации рабочей станции. Предотвращение сбоев в работе в ОС.
4	Антивирусная защита компьютерных систем	Антивирусная защита компьютерных систем. Классификация и возможности вредоносных программ. Меры антивирусной профилактики и уменьшения последствий вирусных атак. Обнаружение и удаление компьютерных вирусов: методы и антивирусные средства. Признаки действия программных закладок и способы их выявления.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-19 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей	У-1 - Проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Комплексное обеспечение защиты информации в объектах информатизации

Электронные ресурсы (издания)

1. Ермаков, , Д. Г.; Применение антивирусных программ для обеспечения информационной безопасности; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2013; http://www.iprbookshop.ru/66577.html (Электронное издание)

Печатные издания

1. Проскурин, В. Г.; Защита программ и данных : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 090900 "Информ. безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информ. безопасность автоматизир. систем".; Академия, Москва; 2011 (25 экз.)

2. Ермаков, Д. Г.; Применение антивирусных программ для обеспечения информационной безопасности : учебное пособие для студентов, обучающихся по программе бакалавриата по направлениям подготовки 080500 "Бизнес-информатика", 230700 "Прикладная информатика", 080100 "Экономика".; Издательство Уральского университета, Екатеринбург; 2013 (10 экз.)

Профессиональные базы данных, информационно-справочные системы

Стандарты - Интернет портал ISO27000.RU http://www.iso27000.ru

http://lib.urfu.ru/mod/data/view.php?id=1379]

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (http:минобрнауки.рф).

Федеральный портал _Российское образование (http:www.edu.ru).

ООО Научная электронная библиотека (http:elibrary.ru).

Зональная научная библиотека УрФУ(http:lib.urfu.ru).

Электронный научный архив УрФУ (https:elar.urfu.ru).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Комплексное обеспечение защиты информации в объектах информатизации

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		санитарными правилами и нормами Подключение к сети Интернет	
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Самостоятельная работа студентов	Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES

		Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
5	Лабораторные занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
6	Курсовая работа/ курсовой проект	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		санитарными правилами и нормами Подключение к сети Интернет	