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
1153522	Безопасность компьютерных систем

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Безопасность компьютерных систем	**Код ОП** 1. 10.03.01/33.01
Направление подготовки 1. Информационная безопасность	**Код направления и уровня подготовки** 1. 10.03.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Золотых Максим Олегович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	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 Безопасность компьютерных систем

1.1. Аннотация содержания модуля

Модуль «Безопасность компьютерных систем» является основополагающим для данного профиля бакалавриата. Модуль содержит в себе дисциплины, излагающие устройство и особенности эксплуатации операционных систем со всеми штатными элементами и службами безопасности. Изучаются основные файловые системы, способы безопасного хранения системных программ и данных, модули аутентификации пользователей, сетевые службы и защищенные технологические режимы. Завершается модуль дисциплиной, излагающей принципы проектирования отечественной ОС Astra Linux.

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	Безопасность компьютерных сетей	3
2	Методы оценки безопасности компьютерных систем	4
3	Администрирование средств защиты информации в компьютерных системах и сетях	4
4	Криптографические протоколы	4
	ИТОГО по модулю:	15

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	1. Методы и средства криптографической защиты информации 2. Комплексное обеспечение защиты информации объекта информатизации

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
Администрирование средств защиты информации в компьютерных системах и сетях	ПК-12 - Способен администрировать средства защиты информации в компьютерных системах и сетях	З-1 - Идентифицировать архитектуры подсистем защиты информации в операционных системах З-2 - Описать принципы построения компьютерных сетей З-3 - Описать принципы функционирования сетевых протоколов, включающих криптографические алгоритмы У-1 - Настраивать антивирусные средства защиты информации в операционных системах У-2 - Устанавливать обновления программного обеспечения и средств антивирусной защиты У-3 - Формировать шаблоны конфигурации программно-аппаратных средств защиты информации в компьютерных сетях П-1 - Выполнять работы по обнаружению вредоносного программного обеспечения П-2 - Выполнять работы ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования П-3 - Выполнять разработку требований к встроенным средствам защиты информации программного обеспечения
	ПК-13 - Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	З-3 - Характеризовать уязвимости используемого программного обеспечения и методы их эксплуатации У-1 - Оценивать угрозы безопасности информации в компьютерных сетях У-2 - Настраивать правила фильтрации пакетов в компьютерных сетях У-3 - Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях П-1 - Определять состава применяемых программно-аппаратных средств защиты информации в операционных системах П-2 - Выполнять разработку порядка применения программно-аппаратных

		средств защиты информации в операционных системах П-3 - Выполнять конфигурирование программно-аппаратных средств защиты информации в операционных системах
Безопасность компьютерных сетей	ПК-13 - Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	З-2 - Описать виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению У-2 - Настраивать правила фильтрации пакетов в компьютерных сетях П-2 - Выполнять разработку порядка применения программно-аппаратных средств защиты информации в операционных системах
	ПК-14 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	З-1 - Описать принципы построения антивирусного программного обеспечения З-2 - Сделать обзор основных средств и методов анализа программных реализаций З-3 - Описать нормативные правовые акты в области защиты информации З-4 - Описать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации У-1 - Анализировать угрозы безопасности информации программного обеспечения У-2 - Формулировать правила безопасной эксплуатации программного обеспечения У-3 - Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия П-1 - Определять состав применяемых программно-аппаратных средств защиты информации в операционных системах П-2 - Определять порядок применения программно-аппаратных средств защиты информации в операционных системах П-3 - Иметь практический опыт формирования шаблонов установки

		программно-аппаратных средств защиты информации в операционных системах П-4 - Определять конфигурацию программно-аппаратных средств защиты информации в операционных системах
Криптографические протоколы	ПК-11 - Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	З-1 - Описать виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению З-2 - Описать принципы функционирования программных средств криптографической защиты информации З-3 - Описать виды политик управления доступом и информационными потоками в компьютерных сетях У-1 - Формулировать политики безопасности операционных систем У-2 - Настраивать политики безопасности операционных систем У-3 - Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях П-1 - Определять порядок установки программного обеспечения с целью соблюдения требований по защите информации П-2 - Контролировать соблюдение требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение П-3 - Выполнять разработку требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения
Методы оценки безопасности компьютерных систем	ПК-14 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и	З-1 - Описать принципы построения антивирусного программного обеспечения З-2 - Сделать обзор основных средств и методов анализа программных реализаций З-3 - Описать нормативные правовые акты в области защиты информации

	корпоративными требованиями	З-4 - Описать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации У-1 - Анализировать угрозы безопасности информации программного обеспечения У-2 - Формулировать правила безопасной эксплуатации программного обеспечения У-3 - Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия П-1 - Определять состав применяемых программно-аппаратных средств защиты информации в операционных системах П-2 - Определять порядок применения программно-аппаратных средств защиты информации в операционных системах П-3 - Иметь практический опыт формирования шаблонов установки программно-аппаратных средств защиты информации в операционных системах П-4 - Определять конфигурацию программно-аппаратных средств защиты информации в операционных системах

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность компьютерных сетей

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	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
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	Модели угроз и информационных нарушителей в компьютерных сетях	Структурные и топологические модели локальных, корпоративных и глобальных компьютерных сетей. Способы перехвата сетевых пакетов в локальной сети. Угрозы безопасности с позиции моноканала. Угрозы с перенаправлением сетевого трафика. Локальная модель сети в топологии шина и звезда. Понятие о сетевом адаптере в режиме беспорядочного (promiscusion) захвата пакетов. Понятие об arp и rarp протоколах. Виды сетевой адресации.
2	Технология и средства межсетевого экранирования	Принципы фильтрации сетевых пакетов. Виды МСЭ. Способы расположения МСЭ в защищаемой сети. Характеристики наиболее известных типов аппаратных МСЭ и их применение. Требования и порядок настройки программных МСЭ в составе ОС Windows и UNIX. Применение стандартных утилит, обеспечивающих МСЭ. Порядок настройки и оценка эффективности персональных МСЭ.
3	Аппаратные средства CISCO	Линейка сетевого оборудования CISCO: изначение, характеристики, внешний вид и применение аппаратных средств CISCO. Инструкция по эксплуатации изделий. Операционная система CISCO. Базовая система команд. , iwconfig, net, netsh, tcpdump, netstat и др., их параметры

4	Сетевые возможности операционных систем Windows, Linux, MacOSX	Сетевые протоколы, реализованные в консольном и графическом режимах. Типовой набор утилит, библиотек, демонов и сценариев сетевого назначения. Утилиты типа ifconfig, ipconfig

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	ПК-12 - Способен администрировать средства защиты информации в компьютерных системах и сетях	З-1 - Идентифицировать архитектуры подсистем защиты информации в операционных системах

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность компьютерных сетей

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. Таненбаум, Леонтьев, А.; Компьютерные сети; Питер, Москва; СПб.; Н. Новгород и др.; 2002 (2 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

Безопасность компьютерных сетей

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	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 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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	**Не требуется**
5	Лабораторные 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 Подключение к сети Интернет	

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы оценки безопасности
компьютерных систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Гибилинда Роман Владимирович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
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:

- **Гибилинда Роман Владимирович, Ассистент,**
- **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	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	целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-14 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	З-2 - Сделать обзор основных средств и методов анализа программных реализаций

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы оценки безопасности компьютерных систем

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 в операционных системах : учебное пособие для студентов вузов, обучающихся по специальностям 10.05.01 -"Компьютерная безопасность", 10.05.03 -"Информационная безопасность автоматизированных систем" и 10.05.04 -"Информационно-аналитические системы безопасности", по направлению подготовки 10.03.01 - "Информационная безопасность", уровень бакалавр.; Горячая линия - Телеком, Москва; 2014 (1 экз.)

2. Степанов, Е. А.; Информационная безопасность и защита информации : Учебное пособие.; ИНФРА-

М, Москва; 2001 (2 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

Методы оценки безопасности компьютерных систем

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 Рабочее место преподавателя	**Не требуется**

		Доска аудиторная 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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Администрирование средств защиты информации в компьютерных системах и сетях

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
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:

- **Куц Дмитрий Владимирович, 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
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 клиент-сервер, 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. Классификация беспроводных систем, анализ состава и архи-тектурных особенностей построения БС, изучение функциональных особенностей современных стандартов БС, проектирование системы информационной безопасности БС на основе моделирования ключе- вых 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. Риск-анализ беспроводных сетей Разработка риск-шанс 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	целенаправленная работа с информацией для использования в практических целях	Технология самостоятельной работы	ПК-12 - Способен администрировать средства защиты информации в компьютерных системах и сетях	З-1 - Идентифицировать архитектуры подсистем защиты информации в операционных системах

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Администрирование средств защиты информации в компьютерных системах и 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. Проскурин, В. Г., Крутов, С. В., Мацкевич, С. В., Мацкевич; Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах : Учеб. пособие для студентов вузов, обучающихся по спец. "Защищенные телекоммуникационные системы", "Орг. и технология защиты информации", "Комплексное обеспечение информ. безопасности автоматизир. систем".; Радио и связь, Москва; 2000 (14 экз.)

2. Ермаков, Д. Г.; Модели, методы и программное обеспечение для построения объединенного Интернет/Интранет сервера организации, обеспечивающего безопасность информационных ресурсов : дис. на соиск. учен. степ. канд. физ.-мат. наук: 05.13.18. ; Екатеринбург; 2005 (1 экз.)

3. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем"....; УГТУ-УПИ, Екатеринбург; 2007 (15 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

Администрирование средств защиты информации в компьютерных системах и 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

		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 Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся	**Не требуется**

		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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические протоколы

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Агафонов Алексей Владимирович	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
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:

- **Агафонов Алексей Владимирович, 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	Общие принципы безопасности операционных систем	Ключевые элементы программной архитектуры операционных систем (ОС), определяющие защиту компьютерной информации и безопасность ЭВМ. Архитектура многозадачной сетевой операционной системы. Уровень ядра и уровень приложений. Объекты ядра. Аппаратно–зависимый программный слой. Защищенные файловые системы. Владение файловыми объектами и права доступа к ним. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Типовые файловые системы. Структура и назначение метаданных файлов. Понятие политики разграничения доступа в

		компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки. Реализация технологии разграничения доступа в операционных системах. Модель безопасности и ее архитектура. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп. Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе. Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС. Безопасность системных данных. Способы защиты системных файлов от незаконной модификации. Управление памятью. Механизмы виртуальной памяти. Создание и уничтожение процессов. Управление процессами и контроль над ними. Реализация многозадачного и многопоточного режимов. Механизмы системных вызовов. Защита на уровне межпроцессного взаимодействия. Сокрытие процессов. Реализация защитных требований на уровне командной оболочки. Защита программного обеспечения от незаконной модификации. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора.
2	Защита компьютерной информации в операционных системах Linux и FreeBSD	Ключевые элементы программной архитектуры ОС, влияющие на защиту информации. Базовые понятия. Основные отличия операционных систем Linux и FreeBSD. Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Основные команды, позволяющие работать с файлами. Действия над обычными файлами: создание, копирование, перемещение, удаление. Работа с каталогами. Создание

		и изменение разрешений на доступ к файлам. Использование «жестких» и символических ссылок. Дополнительные атрибуты файлов, поддерживаемые в ОС Linux. Работа со специальными файлами устройств. Загрузчики операционных систем LILO, GRUB. Обеспечение защиты от НСД при загрузке ОС. Вход в систему в однопользовательском режиме. Загрузка ПК с LiveCD с целью устранения неполадок. Архитектура файловых систем ext*fs и ufs*. Размещение элементов файловой системы на дисковом пространстве. Назначение и структура суперблока, описателей групп блоков, карт битовых полей, индексных дескрипторов, журнала транзакций. Структура индексного дескриптора регулярного файла, каталога, символической ссылки. Работа с устройствами дисковой и полупроводниковой памяти. Создание, изменение и удаление дисковых разделов. Отображение информации о дисковых разделах и файловых системах. Форматирование разделов и создание файловых систем. Конфигурационный файл /etc/fstab. Монтирование устройств и дисковых разделов с различными файловыми системами. Размещение файловых систем на дисковом пространстве. Монтирование разделов памяти с различными файловыми системами. Установление дисковых квот. Восстановление логически удаленных или поврежденных файлов. Последовательность логического удаления файлов в файловых системах ext*fs и ufs*. Виды повреждений файловой системы. Утилиты для работы с поврежденными файловыми системами. Возможности дисковых редакторов типа Linux Disk Editor и отладчиков файловых систем для восстановления утерянной компьютерной информации. Особенности восстановления файлов в различных файловых системах. Использование записей из

		журнальных файлов. Блочное копирование информации с поврежденных машинных носителей с помощью утилиты dd. Ключевые аргументы командной строки. Сетевое копирование с использованием утилиты netcat. Атрибуты процесса. Файловая система /proc как «зеркало» процессов. Переменные окружения. Создание и уничтожение процессов, изменение их приоритетов. Способы автоматического запуска и остановки программ. Периодически запускаемые процессы. Запуск и остановка программ в интерактивном и фоновом режимах. Средства взаимодействия между процессами. Перенаправление ввода/вывода. Терминальный режим и консольные атаки. Вывод информации о процессах. Наблюдение за процессами и контроль производительности системы. Признаки камуфляжа несанкционированно выполняемых процессов. Программные возможности сокрытия процессов. Использование возможностей командных оболочек 7 при решении штатных задач администрирования. Типовой синтаксис команд. Запуск программ в фоновом режиме. Запуск нескольких команд, в т.ч. по условию. Командные файлы. Перенаправление ввода и вывода. Конвейеры. Управление операционной системой в многотерминальном режиме. Работа с файловым менеджером Midnight Commander. Пользователи и их виды. Группы пользователей. Учетные записи пользователей и работа с ними. Изменение, редактирование, удаление и временное блокирование учетных записей. Конфигурационные файлы group, passwd, master.passwd, shadow, login.defs. Временные отметки и признаки паролей. Смена паролей. Процедура регистрации и ее безопасность. Смена пользователей. Предоставление эффективных прав доступа. Использование механизма SUDO.

		Практические задачи на разграничение доступа и их решения. Предоставление пользователям временных прав суперпользователя. Распространенные атаки на права администратора системы. Исследование учетных записей пользователей. Обнаружение неавторизованных учетных записей пользователей и групп. Копирование и запись данных. Архивация и резервирование. Сетевые возможности операционных систем. Контроль и настройка сетевых интерфейсов. Разведка узлов компьютерной сети и сетевых служб. Методы сканирования узлов ЛВС. Возможности утилиты nmap. Режимы открытого и скрытного сканирования. Перехват и анализ сетевого трафика с помощью утилиты tcpdump. Задание условий фильтрации трафика. Особенности настройки и проверки работоспособности узлов беспроводных сетей. Уязвимости алгоритмов криптографической защиты. Наблюдение и аудит в ОС Linux и FreeBSD. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов. Наблюдение за процессами и пользователями. Отслеживание взаимосвязей между субъектами, процессами и объектами. Аудит событий и его безопасность. Системные протоколы, их расположение и заполнение. Источники, потребители и уровни значимости сообщений. Защита системы протоколирования событий. Основные ошибки и просчеты в администрировании компьютерных сетей под управлением операционных систем Linux и FreeBSD. Анализ настроек безопасности UNIX-систем
3	Защита компьютерной информации в операционных системах семейства Windows	Реализация технологии разграничения доступа в ОС Windows *. Объекты и субъекты доступа. Права и методы доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Структура маркера доступа. Процесс

		проверки подлинности при входе в систему. Стратегия предоставления прав на доступ к ресурсам. Защита данных средствами разрешений файловой системы NTFS. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows*. Методы идентификации и аутентификации пользователей, применяемые в ОС Windows*. Криптографическая защита пользовательских данных средствами шифрующей файловой системы EFS. Структура зашифрованного файла. Создание ключа и сертификата агента восстановления. Хранение парольной информации. Анализ уязвимости паролей пользователей. Алгоритмы локальной и сетевой аутентификации. Механизмы криптографической защиты данных на логических разделах и съемных носителях информации, реализованные в ОС Windows 7. Технология BitLocker. Создание замкнутой программной среды с помощью функции AppLocker. Организация файловой системы NTFS. Основные свойства файловой системы NTFS. Структура MFT. Стандартные атрибуты файлов и каталогов в NTFS. Основные операции над объектами файловой системы. Резидентные и нерезидентные атрибуты. Потоки. Структура каталогов. Размещение файловой системы на дисковом пространстве. Разграничение доступа в ОС Windows*. Планирование и создание учетных записей пользователей и рабочих групп. Разграничение доступа к ресурсам. Разрешения доступа к общим папкам. Получение доступа к пользовательским данным с правами администратора. Структура системного реестра ОС Windows*. Редактирование реестра. Разделы и настройки системного реестра, определяющие политику

		безопасности. Использование реестра для настройки параметров ОС. Утилиты администрирования реестра с интерфейсом командной строки. Анализ и настройка политики безопасности. Анализ параметров безопасности. Рекомендуемые права пользователей. Управление системной политикой безопасности. Политика учетных записей. Разработка шаблона политики безопасности. Анализ и настройка политики безопасности с применением шаблонов. Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора. Настройки журнала аудита. Анализ и восстановление данных на логических разделах NTFS. Подключение машинных носителей с NTFS-разделами. Восстановление главной загрузочной записи. Восстановление таблицы разделов и загрузочного сектора. Приемы и программное обеспечение для «ручного» восстановления удаленных файлов на NTFS разделах. Возможности автоматизированного восстановления удаленных файлов. Анализ сетевых служб Windows*. Анализ сетевых компьютеров с использованием стандартных сетевых команд. Анализ сетевых узлов с использованием программ-сканеров портов. Анализ возможности сетевого подключения к файловым ресурсам Windows*. Использование инструментальных средств аудита безопасности компьютерных систем.
4	Особенности защиты компьютерной информации в операционной системе Mac OS X	Создание, изменение и удаление учетных записей пользователей. Регистрация в системе и выход из нее. Включение и использование учетной записи суперпользователя root. Виды паролей: пароль учетной записи, пароль администратора, мастер-пароль, пароль суперпользователя. Выбор паролей с помощью Password Assistant.

		Пароли в виде «связки ключей». Сброс и обновление паролей. Аппаратный пароль Firmware Password. Работа с файлами. Надежное удаление файлов. Права доступа к файлам. Запрет изменений файлов. Особенности файловой системы hfsplus. Структура файлов. Восстановление поврежденных файлов. Использование механизма SUDO для предоставления пользователям дополнительных прав. Системные настройки безопасности. Шифрование пользовательских данных с помощью FileVault. Включение и выключение механизма шифрования. Недостатки режима шифрования. Контроль за режимом изоляции программной среды. Системная защита от вредоносных программ и сетевых атак. Загрузка операционной системы в однопользовательском режиме. Защита компьютеров Apple от непосредственного доступа. Экранная заставка. Контроль рабочего места с помощью видеорегистрации. Настройка средств сетевой защиты Mac OS X 10.6. Особенности регистрации системных событий. Расположение и безопасность журналов аудита

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-	Технология формирования уверенности и	ПК-11 - Способен разрабатывать и реализовывать	З-1 - Описать виды политик управления

	исследовательская	готовности к самостоятельной успешной профессиональной деятельности	политики управления доступом в компьютерных системах	доступом и информационным и потоками применительно к прикладному программному обеспечению

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические протоколы

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. , Синадский, Н. И.; Защита информации в компьютерных сетях : практ. курс.; УГТУ-УПИ, Екатеринбург; 2008 (2 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/defaultx.asp).

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

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

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографические протоколы

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	Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet. Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Консультации	Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		с выходом в глобальную сеть Internet. Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.	
3	Самостоятельная работа студентов	Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet. Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.	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 Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с	**Не требуется**

		санитарными правилами и нормами	
5	Лабораторные занятия	Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet. Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES