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
1156876	Защита информации в объектах критической информационной инфраструктуры (КИИ)

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	Доцент	
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 в объектах критической информационной инфраструктуры (КИИ)

1.1. Аннотация содержания модуля

Целью модуля является формирование знаний и умений в области противодействия компьютерной преступности, решения задач в области в области установки, настройки и эксплуатации систем обнаружения компьютерных атак на значимых объектах критической информационной инфраструктуры далее КИИ , реагирования на компьютерные инциденты на значимых объектах КИИ, а также проектирования базы правил для обнаружения и предупреждения направленных компьютерных атак, формирование рекомендаций по принятию мер, направленных на недопущение повторений подобных инцидентов в будущем. информационной инфраструктуры. В модуле изучаются основные подходы к организации экспертно аналитической деятельности в сфере обеспечения безопасности объектов КИИ принципы аналитической работы с системами обнаружения атак далее —СОА при помощи систем управления базами данных далее —СУБД стандарты и нормативные правовые акты, описывающие порядок реагирования на компьютерные инциденты на значимых объектах КИИ требования, предъявляемые к системам обнаружения компьютерных атак при защите значимых объектов КИИ механизмы компьютерного следообразования принципы функционирования и построения систем обнаружения компьютерных атак ликвидация последствий компьютерного инцидента и совершенствование применяемых мер 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	Методы и средства защиты информации в объектах КИИ	4
2	Безопасность файловых систем	3
3	Расследование инцидентов в области информационной безопасности	3
	ИТОГО по модулю:	10

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Защита информации
Постреквизиты и кореквизиты модуля	1. Проектирование защищенных телекоммуникационных 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
Безопасность файловых систем	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа
	ОПК-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях У-1 - Анализировать защищенность информации от несанкционированного доступа в телекоммуникационных системах и сетях П-1 - Проводить инструментальный мониторинг качества обслуживания от несанкционированного доступа
Методы и средства защиты информации в объектах КИИ	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа

	ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа
	ОПК-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях У-1 - Анализировать защищенность информации от несанкционированного доступа в телекоммуникационных системах и сетях П-1 - Проводить инструментальный мониторинг качества обслуживания от несанкционированного доступа
Расследование инцидентов в области информационной безопасности	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации У-1 - Систематизировать и классифицировать организационно-распорядительные документы,

	Российской Федерации, Федеральной службы по техническому и экспортному контролю	регламентирующие защиту информации ограниченного доступа в автоматизированных системах П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа
	ОПК-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях У-1 - Анализировать защищенность информации от несанкционированного доступа в телекоммуникационных системах и сетях П-1 - Проводить инструментальный мониторинг качества обслуживания от несанкционированного доступа
	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
Методы и средства защиты информации в объектах КИИ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, Старший преподаватель,**

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 сведения о системах	Введение. Цели, задачи и структура курса. Основные понятия и определения. Структура системы передачи сообщений. Количественные характеристики источников информации. Особенности образования и характеристики речевых сигналов. Определение и классификация сигналов. Обобщенные спектральные представления сигналов. Преобразование типа сигнала. Виды и особенности формирования первичных сигналов связи. Основные характеристики первичных сигналов. Согласование сигнала с каналом связи. Корреляционные и спектральные характеристики сигналов. Методы аналого-цифрового преобразования сигналов. Общие сведения о системах

2	Кодирование источников сообщений и сигналов в системах передачи информации. Основные методы модуляции и демодуляции аналоговых и дискретных сигналов при передаче в каналах связи	Основные понятия и классификация методов кодирования. Кодирование источника и кодирование сигнала в канале с шумами. Основы экономного кодирования. Избыточность и относительная скорость кода. Дискретные источники без памяти. Примитивное (безызбыточное) кодирование. Принципы статистического кодирования. Основы помехоустойчивого кодирования. Линейные блочные коды, порождающие матрицы. Декодирование линейных кодов. Проверочные матрицы. Циклические коды. Сверточные (решетчатые) коды. Блочные корректирующие коды. Обнаружение и исправление ошибок. Алгоритмы декодирования. Применение корректирующего кодирования в системах передачи информации. Виды модуляции: основные понятия и определения. Сигналы при непрерывной модуляции: амплитудная и угловая модуляции, их разновидности. Методы импульсной модуляции при передаче непрерывных сообщений: амплитудно-импульсная модуляция, широтно-импульсная модуляция, время-импульсная модуляция структура спектра, связь с параметрами сообщения, принципы демодуляции. Сигналы при дискретной модуляции: амплитудная манипуляция, частотная манипуляция, фазовая манипуляция, квадратурная амплитудная манипуляция. Методы модуляции с расширением спектра. Системы с прямым расширением спектра и па основе псевдослучайной (программной) перестройки рабочей частоты (ППРЧ).
3	Математические модели каналов передачи информации.	Классификация каналов передачи информации. Случайные линейные каналы и их характеристики, особенности проводных и радиоканалов, замирания сигналов. Флуктуационные, сосредоточенные и

		импульсные помехи, их вероятностные характеристики. Модели непрерывных каналов. Модели дискретного канала. Модели волоконно- оптических каналов связи. Марковские модели каналов. Уравнение состояния и наблюдения в скалярной и векторной форме. Моделирование каналов на основе метода переменных состояний.

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-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы и средства защиты информации в объектах КИИ

Электронные ресурсы (издания)

1. Башлы, П. Н.; Информационная безопасность: учебно-практическое пособие : учебное пособие.; Евразийский открытый институт, Москва; 2011; https://biblioclub.ru/index.php?page=book&id=90539 (Электронное издание)

Печатные издания

1. Гаранин, М. В., Журавлев, В. И., Кунегин, С. В.; Системы и сети передачи информации : Учеб. пособие для студентов вузов, обучающихся по специальностям "Криптография", "Компьютерная безопасность", "Комплексное обеспечение информац. безопасности автоматизир. систем", "Информац. безопасность телекоммуникац. систем".; Радио и связь, Москва; 2001 (21 экз.)

2. Прозоров, В. М., Стебленко, А. И., Абилов, А. В.; Общеканальная система сигнализации N 7 : учеб. пособие для студентов вузов, обучающихся по специальностям 200900 (210406) - "Сети связи и системы коммутации", 201000 (210404) - "Многоканал. телекоммуникац. системы", 201200 (210402) - "Средства связи с подвиж. объектами".; Горячая линия - Телеком, Москва; 2008 (10 экз.)

Профессиональные базы данных, информационно-справочные системы

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

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

1. Министерство образования науки Российской Федерации (http:_минобрнауки.рф_)

2. Федеральный портал_ Российское образование_(http:_ www.edu.ru_)

3. ООО Научная электронная библиотека (http:_elibrary.ru_defaultx.asp)

4. Зональная научная библиотека УрФУ (http:_lib.urfu.ru)

5. Электронный научный архив УрФУ (http:_elar.urfu.ru_)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Методы и средства защиты информации в объектах КИИ

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	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		комплекс межсетевого экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	
2	Практические занятия	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		комплекс межсетевого экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	
5	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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность файловых систем

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	Доцент	

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

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	Технологии хранения данных	Технология хранения данных. Логика хранения данных. Причины потерь информации. Виды потерь информации. Защита и безопасность данных
2	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
3	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
4	Безопасное хранение резервных копий	Настройка политики хранения данных. Выбор ПО, оборудования и сайтов. Сжатие и дедупликация данных. Оценка стоимости хранения
5	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
6	Управление резервным копированием	Возможности резервного копирования. Оптимальный план восстановления и проверка его эффективности. Отслеживание исполнения плана резервирования данных. Настройка окна резервного копирования.

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	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа

			службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
			ОПК-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность файловых систем

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. 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, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

2. 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.)

3. Князева; Разработка методики идентификации последовательности внешних воздействий на

динамическую систему, изоморфную конечному автомату (на примере восстановления последовательности файловых операций в операционной системе) : специальность 2.3.1 - Системный анализ, управление и обработка информации. ; Екатеринбург; 2021 (1 экз.)

4. Воеводин, С. В.; Системы охранного телевидения : учебное пособие для студентов вузов, обучающихся по направлению подготовки 210400-Радиотехника в УрФО.; Издательство Уральского университета, Екатеринбург; 2013 (5 экз.)

5. Гибилинда; Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности : специальность 2.3.6 - Методы и системы защиты информации, информационная безопасность. ; Екатеринбург; 2021 (1 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

1. Министерство образования науки Российской Федерации (http:_минобрнауки.рф_)

2. Федеральный портал_ Российское образование_(http:_ www.edu.ru_)

3. ООО Научная электронная библиотека (http:_elibrary.ru_defaultx.asp)

4. Зональная научная библиотека УрФУ (http:_lib.urfu.ru)

5. Электронный научный архив УрФУ (http:_elar.urfu.ru_)

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность файловых 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	Office 365 EDUA1 ShrdSvr ALNG SubsVL MVL PerUsr Student EES

		Доска аудиторная Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	
2	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
3	Консультации	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 санитарными правилами и нормами	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	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		Доска аудиторная Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
5	Самостоятельная работа студентов	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
Расследование инцидентов в области информационной безопасности

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	
2	Князева Наталия Сергеевна	кандидат технических наук, без ученого звания	Доцент	

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

Протокол № _9_ от _21.09.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

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	Судебная компьютерно-техническая экспертиза (СКТЭ)	История возникновения СКТЭ, определение и объекты СКТЭ, видовая классификация (аппаратно-компьютерная экспертиза, программно-компьютерная экспертиза, информационно-компьютерная экспертиза, компьютерно-сетевая экспертиза), этапы проведения исследования, методы и инструменты СКТЭ, эксперт (статья 57 УПК РФ), заключение эксперта (статья 204 УПК РФ).
2	Особенности компьютерного следообразования в ОС Windows	Системные следообразующие факторы в ОС Windows, компьютерные следы, следовоспринимающие объекты в ОС Windows (файлы системного реестра, системные журналы, служебные файлы, файл гибернации, файл подкачки), методика исследования механизмов следообразования в ОС Windows.
3	Следы в ОС Windows	Места фиксирования следов установки и запуска программ, подключения USB-устройств, подключения к сети Интернет, служба Superfetch, механизм идентификации USB-устройств.
4	Ретроспективный анализ	Форматы представления временных отметок, временные отметки в таблице MFT, проведение ретроспективного анализа по соотношениям временных отметок, структура ярлыка, события, фиксирующиеся в системных журналах, представляющие интерес для ретроспективного анализа.
5	Подбор паролей	Способы восстановления паролей, атака перебором, атака по словарю, формирование собственного словаря, возможные

		модификации слов в словаре, атака по маске, комбинированная атака, рекомендации по подбору паролей.
6	Информационный поиск	Сигнатурный поиск, контекстный поиск, поиск по хэш-значениям, объекты и инструменты поиска, применение индексирования при поиске.
7	Контр-форензика	Программы и аппаратно-программные устройства для шифрования хранимой информации и шифрования трафика, программы для очистки дисков и других носителей, программы для удаления «конфиденциальной» информации пользователя, устройства для механического уничтожения информации на носителях информации.
8	Исследование и преобразование системного реестра ОС Windows	Общие сведения о системном реестре, структура файла улья, структура ячейки раздела, списка разделов, списка параметров, параметра, значения параметра, алгоритм восстановления удаленных разделов, программа для работы с реестром, программы чистки и оптимизации реестра.
9	Мобильная криминалистика	Что такое криминалистика мобильных устройств, проблемы мобильной криминалистики, исследование мобильных устройств, обзор операционных систем мобильных устройств, методы извлечения данных и выбор инструментария, потенциальные доказательства, хранящиеся на мобильных устройствах.

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	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа

			Российской Федерации, Федеральной службы по техническому и экспортному контролю	
			ОПК-15 - Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	З-1 - Описывать особенности инструментального мониторинга качества обслуживания в телекоммуникационных системах и сетях

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Расследование инцидентов в области информационной безопасности

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. Гибилинда; Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности : специальность 2.3.6 - Методы и системы защиты информации, информационная безопасность. ; Екатеринбург; 2021 (1 экз.)

2. 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, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 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.)

4. Синадский, Н. И., Бакланов, В. В.; Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие.; [ГОУ ВПО УГТУ-УПИ], Екатеринбург; 2007 (70 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

Расследование инцидентов в области информационной безопасности

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 Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES

2	Лабораторные занятия	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 санитарными правилами и нормами Подключение к сети Интернет	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES
3	Консультации	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 санитарными правилами и нормами	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student 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	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES

		санитарными правилами и нормами Подключение к сети Интернет	
5	Самостоятельная работа студентов	Доска аудиторная Персональные компьютеры по количеству обучающихся Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	Office 365 ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsr STUUseBnft Student EES