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 |
|---|---|
| 1156882 | Проектирование защищенных телекоммуникационных систем |

**Екатеринбург**

| Перечень сведений о рабочей программе модуля | Учетные данные |
|---|---|
| **Образовательная программа**<br>1. Информационная безопасность телекоммуникационных систем | **Код ОП**<br>1. 10.05.02/22.01 |
| **Направление подготовки**<br>1. Информационная безопасность телекоммуникационных систем | **Код направления и уровня подготовки**<br>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 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

**Согласовано:**

Управление образовательных программ Р.Х. Токарева

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Проектирование защищенных телекоммуникационных систем

## 1.1. Аннотация содержания модуля

В рамках модуля «Проектирование защищенных телекоммуникационных систем» рассматриваются принципы построения, функционирования использования компьютерных сетей различного масштаба, возможностей их реализации на основе базовых технологий и стандартов. Также рассматриваются вопросы взаимодействия компьютеров и сетевого оборудования на программном и аппаратном уровнях.

## 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 | Проектирование защищенных телекоммуникационных систем | 4 |
| | ИТОГО по модулю: | 4 |

## 1.3.Последовательность освоения модуля в образовательной программе

| | |
|---|---|
| **Пререквизиты модуля** | 1. Защита информации |
| **Постреквизиты и кореквизиты модуля** | 1. Защита информации в информационно-управляющих систем |

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

Таблица 2

| Перечень дисциплин модуля | Код и наименование компетенции | Планируемые результаты обучения (индикаторы) |
|---|---|---|
| 1 | 2 | 3 |
| Проектирование защищенных телекоммуникационных систем | ОПК-9 - Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач | З-1 - Идентифицировать профессиональную и криптографическую терминологию в области безопасности информации<br>З-2 - Объяснять основные информационные технологии, используемые в автоматизированных системах |

| | | |
|---|---|---|
| | профессиональной деятельности | З-3 - Объяснять основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах<br><br>З-4 - Различать принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br><br>У-1 - Оценивать сложность алгоритмов и вычислений<br><br>У-2 - Проводить комплексное тестирование аппаратных и программных средств<br><br>П-1 - Разрабатывать техническую документацию в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем<br><br>П-2 - Разрабатывать программное обеспечение, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации<br><br>П-3 - Оптимизировать работу электронных схем с учетом требований по защите информации |
| | ПК-4 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем | З-1 - Характеризовать основные информационные технологии, используемые в автоматизированных системах<br><br>З-2 - Характеризовать средства и способы обеспечения безопасности информации, принципы построения систем защиты информации<br><br>У-1 - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |

| | | |
|---|---|---|
| | | П-1 - Иметь опыт практической разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации |
| | ПК-5 - Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа | З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД<br><br>З-2 - Характеризовать современные информационные технологии (операционные системы, базы данных, вычислительные сети)<br><br>З-3 - Характеризовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах<br><br>З-4 - Различать основные классы и виды уязвимостей программного обеспечения<br><br>З-5 - Объяснять методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее<br><br>З-6 - Характеризовать (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее<br><br>З-7 - Характеризовать методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий<br><br>З-8 - Характеризовать средства контроля защищенности информации от несанкционированного доступа<br><br>З-9 - Характеризовать методики контроля защищенности информации от несанкционированного доступа<br><br>З-10 - Характеризовать средства проектирования электронных схем<br><br>У-1 - Составлять техническое задание на создание программно-технического средства защиты информации от |

| | | |
|---|---|---|
| | | несанкционированного доступа и специальных воздействий на нее<br><br>У-2 - Составлять проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее<br><br>У-3 - Составлять программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее<br><br>П-1 - Иметь опыт практической разработки технического (эскизного) проекта программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее<br><br>П-2 - Иметь опыт практического испытания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее<br><br>П-3 - Иметь опыт практической разработки рабочей и эксплуатационной документации на техническое средство защиты |

**1.5. Форма обучения**

Обучение по дисциплинам модуля может осуществляться в очной формах.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
**Проектирование защищенных телекоммуникационных систем**

Рабочая программа дисциплины составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Пономарева Ольга Алексеевна | кандидат технических наук, без ученого звания | Доцент | |
| 2 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

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

Протокол № _9_ от _21.09.2021_ г.

## 1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**Авторы:**

- **Пономарева Ольга Алексеевна, Старший преподаватель,**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

### 1.1. Технологии реализации, используемые при изучении дисциплины модуля

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

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

### 1.2. Содержание дисциплины

Таблица 1.1

| Код раздела, темы | Раздел, тема дисциплины* | Содержание |
|---|---|---|
| **1** | Управление инцидентами информационной безопасности | Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ. |
| **2** | Сбор и анализ технических данных при реагировании на инциденты | Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ:  сбор технических данных с компонентов информационной инфраструктуры;  поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению;  распространение (передача) выделенной и оформленной содержательной (семантической) информации; |

| | | |
|---|---|---|
| | | □ обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры.<br>Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации об инциденте ИБ; содержание информации об инциденте ИБ, полученной от источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет.<br>Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных.<br>Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем.<br>Копирование протоколов (журналов) регистрации. Копирование сетевого трафика. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. Структура протокола обработки технических данных.<br>Технические средства и инструменты для сбора и обработки технических данных: 6 технические средства выполнения криминалистической копии (создания образа) запоминающих устройств и содержимого оперативной памяти СВТ; технические средства получения данных операционных систем о сетевых конфигурациях, о сетевых соединениях, об |

| | | |
|---|---|---|
| | | открытых файлах, о запущенных процессах, об открытых сессиях доступа.» |
| **3** | Обеспечение режима защиты информации персональных данных (ПДн), и безопасности ПДн в организации | Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных».<br>Меры, по обеспечению безопасности ПДн при их обработке.<br>Понятие угроз безопасности ПДн.<br>Определение уровня защищенности ПДн |

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-9 - Способен использовать программные, программно-аппаратные и технические средства защиты информации при решении задач профессиональной деятельности | У-2 - Проводить комплексное тестирование аппаратных и программных средств |

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Проектирование защищенных телекоммуникационных систем**

**Электронные ресурсы (издания)**

1. Галатенко, В. А., Бетелин, В. Б.; Основы информационной безопасности: Курс лекций : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Москва; 2006; https://biblioclub.ru/index.php?page=book&id=233063 (Электронное издание)

2. , 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. Бакланов, В. В.; Введение в информационную безопасность. Направления информационной защиты : курс лекций.; Изд-во Уральского университета, Екатеринбург; 2007 (3 экз.)

2. , Белов, Е. Б., Лось, В. П., Мещеряков, Р. В., Шелупанов, А. А.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности.; Горячая линия - Телеком, Москва; 2006 (26 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, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

4. 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.)

5. 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

**Проектирование защищенных телекоммуникационных 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 | Лабораторные занятия | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Персональные компьютеры по количеству обучающихся<br>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами<br>Подключение к сети Интернет | Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES |
| 2 | Текущий контроль и промежуточная аттестация | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Персональные компьютеры по количеству обучающихся<br>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами<br>Подключение к сети Интернет | Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES |
| 3 | Лекции | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с | **Не требуется** |

| | | | |
|---|---|---|---|
| | | санитарными правилами и нормами | |
| 4 | Консультации | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами | **Не требуется** |
| 5 | Самостоятельная работа студентов | Персональные компьютеры по количеству обучающихся<br>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами<br>Подключение к сети Интернет | Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES |