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 |
|---|---|
| 1157342 | Средства и методы защиты информации |

**Екатеринбург**

| Перечень сведений о рабочей программе модуля | Учетные данные |
|---|---|
| **Образовательная программа**<br>1. Математические методы защиты информации | **Код ОП**<br>1. 10.05.01/22.01 |
| **Направление подготовки**<br>1. Компьютерная безопасность | **Код направления и уровня подготовки**<br>1. 10.05.01 |

Программа модуля составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Баранский Виталий Анатольевич | доктор физико-математических наук, профессор | Профессор | алгебры и фундаментальной информатики |
| 2 | Богданов Валентин Викторович | кандидат технических наук, без ученого звания | Доцент | алгебры и фундаментальной информатики |
| 3 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

**Согласовано:**

Управление образовательных программ Р.Х. Токарева

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Средства и методы защиты информации

## 1.1. Аннотация содержания модуля

Модуль «Средства и методы защиты информации» предполагает получение студентами компетенций по установке, наладке, тестированию и обслуживанию современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. В модуль входят следующие дисциплины: «Криптографические протоколы», «Защита программ и данных», «Программно-аппаратные средства обеспечения информационной безопасности», «Основы построения защищённых компьютерных сетей»

## 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 | Защита программ и данных | 2 |
| 2 | Криптографические протоколы | 3 |
| 3 | Основы построения защищённых компьютерных сетей | 7 |
| 4 | Программно-аппаратные средства обеспечения информационной безопасности | 7 |
| | ИТОГО по модулю: | 19 |

## 1.3.Последовательность освоения модуля в образовательной программе

| | |
|---|---|
| **Пререквизиты модуля** | 1. Криптографические методы защиты информации |
| **Постреквизиты и кореквизиты модуля** | Не предусмотрены |

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

Таблица 2

| Перечень дисциплин модуля | Код и наименование компетенции | Планируемые результаты обучения (индикаторы) |
|---|---|---|
| 1 | 2 | 3 |

| | | |
|---|---|---|
| Защита программ и данных | ОПК-13 - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности | З-1 - Перечислить основные средства защиты машинных носителей информации от непосредственного доступа<br><br>З-2 - Изложить общие принципы построения программно-алгоритмических средств защиты информации в сложных клиентских приложениях<br><br>З-5 - Описывать объекты защиты и угрозы безопасности информации<br><br>У-1 - Анализировать и правильно использовать защитные механизмы, внедренные на прикладном программном уровне<br><br>У-2 - Оценивать и контролировать эффективность мер защиты<br><br>У-4 - Оценивать и контролировать эффективность мер защиты<br><br>П-2 - Иметь практический опыт администрирования безопасности защищенных компьютерных систем |
| | ОПК-14 - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации | З-1 - Перечислить основные средства защиты машинных носителей информации от непосредственного доступа<br><br>У-1 - Оценивать и контролировать эффективность мер защиты<br><br>У-2 - Организовать защиту баз данных в различных системах управления<br><br>П-1 - Иметь практический опыт работы с технологией организации защиты информации применительно к конкретным СУБД и базам данных |
| | ПК-6 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем | З-1 - Изложить профессиональную и криптографическую терминологию в области безопасности информации<br><br>З-2 - Характеризовать основные информационные технологии, используемые в автоматизированных системах<br><br>З-3 - Характеризовать средства и способы обеспечения безопасности информации, принципы построения систем защиты информации |

| | | |
|---|---|---|
| | | З-4 - Характеризовать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах<br><br>У-2 - Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД<br><br>У-3 - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах<br><br>У-4 - Проводить комплексное тестирование аппаратных и программных средств<br><br>П-1 - Выполнять разработку технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем<br><br>П-4 - Выполнять разработку программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации<br><br>П-5 - Выполнять разработку электронных схем с учетом требований по защите информации<br><br>П-6 - Иметь практический опыт оптимизации работы электронных схем с учетом требований по защите информации |
| | ПК-7 - Способен разрабатывать компоненты системы управления базами данных | З-9 - Объяснять методы повышения надежности работы системы управления базами данных<br><br>З-13 - Характеризовать способы и механизмы управления данными |

| | | |
|---|---|---|
| | | З-16 - Объяснять методы организации файловых систем<br><br>З-24 - Объяснять основы информационной безопасности<br><br>З-26 - Воспроизвести локальные нормативные правовые акты, действующие в организации<br><br>У-7 - Применять нормативно-техническую документацию при использовании систем управления базами данных<br><br>П-1 - Иметь практический опыт получения технической документации на разработку системы управления базами данных<br><br>П-2 - Иметь практический опыт изучения технической документации на разработку системы управления базами данных<br><br>П-9 - Выполнять разработку системы контроля целостности данных<br><br>П-11 - Выполнять разработку системы резервного копирования<br><br>П-12 - Иметь практический опыт написания исходного кода системы управления базами данных на языке программирования системы управления базами данных<br><br>П-13 - Иметь практический опыт передачи исходного кода системы управления базами данных на тестирование |
| Криптографические протоколы | ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | З-1 - Классифицировать и дать общую характеристику основных типов криптографических протоколов<br><br>З-2 - Описывать основные принципы построения и особенности реализации криптографических протоколов<br><br>З-3 - Описывать способы решения основных задач современной криптографии<br><br>У-1 - Оценивать механизмы защиты, реализующие криптографические протоколы<br><br>У-2 - Оценивать и контролировать эффективность криптографических протоколов |

| | | |
|---|---|---|
| | | У-5 - Реализовывать алгоритмы идентификации с нулевым разглашением<br><br>П-1 - Разрабатывать компоненты криптографических протоколов |
| | ОПК-18 - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации | З-5 - Классифицировать и дать общую характеристику основных типов криптографических протоколов<br><br>З-6 - Описывать основные принципы построения и особенности реализации криптографических протоколов<br><br>З-7 - Описывать способы решения основных задач современной криптографии<br><br>У-1 - Оценивать механизмы защиты, реализующие криптографические протоколы<br><br>У-2 - Оценивать и контролировать эффективность криптографических протоколов<br><br>У-5 - Реализовывать алгоритмы идентификации с нулевым разглашением<br><br>П-2 - Разрабатывать компоненты криптографических протоколов |
| | ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | З-7 - Описывать криптографические протоколы, применяемые в компьютерных сетях |
| Основы построения защищённых компьютерных сетей | ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях | З-2 - Перечислить основные принципы построения защищенных компьютерных систем<br><br>З-4 - Классифицировать вредоносные программы и компоненты информационного оружия<br><br>У-2 - Оценивать и контролировать эффективность мер защиты разрабатывать компоненты программно-аппаратных комплексов защиты информации<br><br>П-1 - Иметь практический опыт проектирования систем защиты |

| | | |
|---|---|---|
| | | информации от несанкционированного доступа |
| | ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | З-1 - Описывать принципы построения компьютерных систем и сетей<br><br>З-2 - Описывать формальные модели безопасности компьютерных систем и сетей<br><br>З-3 - Описывать принципы построения систем обнаружения компьютерных атак<br><br>З-4 - Объяснять методы обработки данных мониторинга безопасности компьютерных систем и сетей<br><br>З-6 - Характеризовать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы<br><br>У-1 - Формализовывать задачу управления безопасностью компьютерных систем<br><br>У-3 - Применять методы анализа защищенности компьютерных систем и сетей<br><br>П-1 - Сделать вывод о защищенности компьютерных систем с использованием сканеров безопасности<br><br>П-2 - Сделать вывод о защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей |
| | ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов | З-1 - Воспроизвести форматы хранения информации в анализируемой компьютерной системе<br><br>З-2 - Воспроизвести основные форматы файлов, используемые в компьютерных системах<br><br>З-3 - Воспроизвести особенности хранения конфигурационной и системной информации в компьютерных системах<br><br>З-4 - Характеризовать уязвимости компьютерных систем и сетей<br><br>З-12 - Объяснять методы анализа систем обеспечения информационной безопасности объектов информатизации на базе |

| | | |
|---|---|---|
| | | компьютерных систем в защищенном исполнении<br><br>У-3 - Определять причину и условия изменения программного обеспечения<br><br>У-5 - Определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой<br><br>П-5 - Сделать вывод о функциональных свойствах программного обеспечения<br><br>П-8 - Иметь практический опыт индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы<br><br>П-9 - Сделать вывод о групповой принадлежности программного обеспечения<br><br>П-10 - Разрабатывать рекомендации по устранению выявленных уязвимостей |
| Программно-аппаратные средства обеспечения информационной безопасности | ОПК-13 - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности | З-1 - Перечислить основные средства защиты машинных носителей информации от непосредственного доступа<br><br>З-3 - Классифицировать и дать общую характеристику программно-аппаратных средств защиты информации<br><br>З-4 - Изложить особенности реализации методов защиты информации программно-аппаратными средствами<br><br>З-5 - Описывать объекты защиты и угрозы безопасности информации<br><br>У-2 - Оценивать и контролировать эффективность мер защиты<br><br>У-3 - Выполнять настройку защитных механизмов программно-аппаратных средств<br><br>У-4 - Оценивать и контролировать эффективность мер защиты<br><br>П-1 - Осуществлять обоснованный выбор современных средствами защиты АС от несанкционированного доступа |

| | | |
|---|---|---|
| | ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях | З-1 - Классифицировать и дать общую характеристику программно-аппаратных средств защиты информации<br><br>З-3 - Характеризовать особенности реализации методов защиты информации программно-аппаратными средствами<br><br>У-1 - Выбирать механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем<br><br>У-2 - Оценивать и контролировать эффективность мер защиты разрабатывать компоненты программно-аппаратных комплексов защиты информации<br><br>П-1 - Иметь практический опыт проектирования систем защиты информации от несанкционированного доступа |
| | ОПК-20 - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов | З-1 - Перечислить основные средства защиты машинных носителей информации от непосредственного доступа<br><br>З-2 - Изложить общие принципы построения программно-алгоритмических средств защиты информации в сложных клиентских приложениях<br><br>З-3 - Классифицировать и дать общую характеристику программно-аппаратных средств защиты информации<br><br>З-4 - Изложить особенности реализации методов защиты информации программно-аппаратными средствами<br><br>З-5 - Описывать объекты защиты и угрозы безопасности информации<br><br>У-1 - Анализировать и правильно использовать защитные механизмы, внедренные на прикладном программном уровне<br><br>У-2 - Оценивать и контролировать эффективность мер защиты<br><br>У-3 - Выполнять настройку защитных механизмов программно-аппаратных средств |

| | | |
|---|---|---|
| | | У-4 - Оценивать и контролировать эффективность мер защиты<br><br>П-1 - Осуществлять обоснованный выбор современных средствами защиты АС от несанкционированного доступа<br><br>П-2 - Осуществлять обоснованный выбор средств администрирования программно-аппаратных комплексов защиты информации |
| | ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации | З-1 - Описывать принципы построения компьютерных систем и сетей<br><br>З-2 - Объяснять методы и методики оценки безопасности программно-аппаратных средств защиты информации<br><br>З-3 - Описывать принципы построения программно-аппаратных средств защиты информации<br><br>З-4 - Описывать принципы построения подсистем защиты информации в компьютерных системах<br><br>З-5 - Объяснять методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации<br><br>З-6 - Объяснять методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации<br><br>З-7 - Объяснять методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей<br><br>З-8 - Характеризовать способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности<br><br>З-12 - Классифицировать организационные меры по защите информации<br><br>У-1 - Определять параметры функционирования программно-аппаратных средств защиты информации |

| | | |
|---|---|---|
| | | У-2 - Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации<br><br>У-3 - Оценивать эффективность защиты информации<br><br>У-4 - Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации<br><br>У-5 - Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия<br><br>П-1 - Сделать вывод о работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик<br><br>П-2 - Сделать вывод об эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик<br><br>П-3 - Сделать вывод об уровне защищенности и доверия программно-аппаратных средств защиты информации |
| | ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | З-1 - Описывать принципы построения компьютерных систем и сетей<br><br>З-10 - Классифицировать организационные меры по защите информации<br><br>У-1 - Формализовывать задачу управления безопасностью компьютерных систем<br><br>У-2 - Применять инструментальные средства проведения мониторинга защищенности компьютерных систем<br><br>П-1 - Сделать вывод о защищенности компьютерных систем с использованием сканеров безопасности<br><br>П-2 - Сделать вывод о защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей |
| | ПК-5 - Способен проводить экспертизы при расследовании | П-1 - Сделать вывод о свойствах аппаратных средств в составе |

| | | |
|---|---|---|
| | компьютерных преступлений, правонарушений и инцидентов | компьютерной системы и их фактическом и первоначальном состоянии<br><br>П-2 - Сделать вывод о свойствах аппаратных средств в составе компьютерной системы |
| | ПК-6 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем | З-1 - Изложить профессиональную и криптографическую терминологию в области безопасности информации<br><br>З-4 - Характеризовать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах<br><br>З-7 - Характеризовать особенности защиты информации в автоматизированных системах управления технологическими процессами<br><br>З-8 - Описывать принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br><br>З-9 - Описывать принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения<br><br>З-10 - Объяснять методы тестирования и отладки программного и аппаратного обеспечения<br><br>З-11 - Описывать архитектуру, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных<br><br>У-2 - Разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД<br><br>У-3 - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей |

| | | |
|---|---|---|
| | | безопасности информации в автоматизированных системах<br><br>П-2 - Иметь практический опыт применения средств схемотехнического проектирования и современной измерительной аппаратуры<br><br>П-3 - Иметь практический опыт синтеза структурных и функциональных схем защищенных автоматизированных систем<br><br>П-5 - Выполнять разработку электронных схем с учетом требований по защите информации |

**1.5. Форма обучения**

Обучение по дисциплинам модуля может осуществляться в очной формах.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
**Защита программ и данных**

Рабочая программа дисциплины составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Бакланов Валентин Викторович | кандидат технических наук, доцент | Доцент | Департамент радиоэлектроники и связи |
| 2 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

**Рекомендовано учебно-методическим советом института** Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

## 1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**Авторы:**

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **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 |
|---|---|---|
| **Р1** | Защита компьютерной информации, хранимой в долговременных устройствах памяти | Понятия о физических принципах и стойкости запечатления компьютерной информации на внешних машинных носителях. Средства записи и считывания информации с машинных носителей. Параметры дисковых накопителей и магнитных носителей, особенности их эксплуатации. Оптические носители информации. Внешняя память на полупроводниковых структурах.<br><br>Общесистемные и специализированные программные средства, и методы логического и физического удаления компьютерной информации, оценка их эффективности. Программные способы удаления хранимой компьютерной информации. Аппаратные устройства мгновенного размагничивания магнитных носителей, их характеристики. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Существующие способы и средства реставрации удаленной компьютерной информации и восстановления поврежденных машинных носителей. Возможности аппаратно-программного комплекса PC–3000. Методы и средства восстановления работоспособности полупроводниковых носителей USBFlash и хранимой на них информации. |

| | | |
|---|---|---|
| **Р2** | Резервирование и архивирование<br>компьютерной информации | Резервирование компьютерной информации как основная мера обеспечения ее сохранности. Порядок хранения и обновления архивных копий. Сравнительные характеристики программ-архиваторов. Виды архивирования. Восстановление системной информации, данных и программного обеспечения с резервных копий. Виды и стратегии резервирования. Использование стандартных средств резервирования системной информации и данных, программ-архиваторов. Устройства и носители, используемые для резервного копирования.<br><br>Организация отказоустойчивых дисковых конфигураций (RAID). Создание зеркальных и дуплексных наборов. Чередование дисков с записью четности. Восстановление информации из зеркальных наборов и наборов с чередованием и контролем четности. |
| **Р3** | Защита компьютерной информации на уровне<br>клиентских программных приложений | Защитные механизмы текстового процессора Microsoft Word. Характеристика офисного пакета как операционной среды для разработки текстовых, графических, табличных и иных документов.<br><br>Механизмы образования технологического информационного мусора, способствующие утечке конфиденциальной информации. Информация, содержащаяся в «Свойствах» и скрытых полях документа. Документ Word как стегоконтейнер. Накопление «мусора» во фрагментах документов и шаблонов. Режим «быстрого сохранения» документов. Способы выявления и удаления скрытых и пользовательских данных.<br><br>Защитные механизмы, реализованные в текстовом процессоре Word. Особенности формата документов и шаблонов. Структура файлов Office XML. Возможности восстановления поврежденных файлов. Уязвимости нового формата Microsoft Word. Шифрование содержимого документа. Ограничение прав пользователей на документы. Защита целостности документов. Использование цифровой подписи и недостатки в ее реализации. Возможности парольной защиты от изменения документа и доступа к встроенному программному коду. Особенности встроенной среды программирования VBA. Программные проекты, модули, процедуры и функции. Событийные процедуры. Автоисполняемые макросы. Приоритет запуска событийных процедур из различных программных модулей в документах и шаблонах. Реализация стандартной защиты от вирусов в макросах. Возможности использования офисных приложений для обработки конфиденциальной информации. |
| **Р4** | Средства обеспечения безопасности баз данных | Средства идентификации и аутентификации объектов баз данных, Языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных. Средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и |

| | | |
|---|---|---|
| | | восстановления баз данных, технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных |

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-6 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем | У-3 - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах |

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Защита программ и данных**

**Электронные ресурсы (издания)**

**Печатные издания**

1. 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.)

2. Гайдамакин, Н. А.; Автоматизированные информационные системы, базы и банки данных. Вводный курс : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем".; Гелиос АРВ, Москва; 2002 (14 экз.)

**Профессиональные базы данных, информационно-справочные системы**

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

2. Бакланов В. В. Программно-аппаратная защита информации / Бакланов В.В., Ваулин С.С., Синадский Н.И. — УМК. — 2007. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7232>.

3. Гайдамакин Н.А. Информационная безопасность АИС, баз и банков данных / Гайдамакин Н.А. — 2008. — Курс "Информационная безопасность АИС, баз и банков данных" является специальным курсом для специальности "Компьютерная безопасность". Излагаются методы и средства защиты информации для автоматизированных информационных систем, баз и банков данных. УМКД включает учебное пособие, программу дисциплины, вопросы для самоконтроля, методические указания, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ . — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11055>.

**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**

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ

http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

## 3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Защита программ и данных**

**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<br>Рабочее место преподавателя<br>Доска аудиторная<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 2 | Практические занятия | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc<br>Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 3 | Консультации | 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>Подключение к сети Интернет | Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc<br>Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 4 | Текущий контроль и промежуточная аттестация | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Периферийное устройство<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc<br>Office Professional 2003 Win32 Russian CD-ROM |
| 5 | Самостоятельная работа студентов | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов | Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc<br>Office Professional 2003 Win32 Russian CD-ROM |

| | | | |
|---|---|---|---|
| | | Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Свободное ПО:Google Crome |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
**Криптографические протоколы**

Рабочая программа дисциплины составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Попов Владимир Юрьевич | доктор физико-математических наук, доцент | Профессор | алгебры и фундаментальной информатики |

**Рекомендовано учебно-методическим советом института** Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

## 1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**Авторы:**

- **Попов Владимир Юрьевич, Профессор, алгебры и фундаментальной информатики**

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

### 1.2. Содержание дисциплины

Таблица 1.1

| Код раздела, темы | Раздел, тема дисциплины* | Содержание |
|---|---|---|
| **Р1** | Введение в криптографические протоколы | Общие сведения о криптографических протоколах. Принципы построения криптографических протоколов. Классификация криптографических протоколов. Методы анализа надежности криптографических протоколов. |
| **Р2** | Идентификация и аутентификация | Типы протоколов идентификации и аутентификации. Методы интегрирования протоколов идентификации и аутентификации в компьютерные системы. |
| **Р3** | Протоколы для работы с ключами | Протоколы обмена ключами. Депонирование ключей и возможность контроля информационного взаимодействия. |
| **Р4** | Протоколы хранения информации | Схемы разделения секрета. Доказательство с нулевым разглашением. |
| **Р5** | Сетевые протоколы | Протоколы широковещания. Системы электронного голосования. Протоколы защиты данных в сети Internet. |
| **Р6** | Графические методы теории криптографических протоколов | Использование графических элементов в сложных многофункциональных протоколах. Визуальные протоколы. Протоколы обмена информацией под наблюдением. |
| **Р7** | Интеллектуальные методы теории криптографических протоколов | Нейросетевые протоколы. Протоколы на основе генетических алгоритмов. Использование интеллектуальных методов при построении и анализе криптографических протоколов. Протоколы квантовой и постквантовой криптографии. |
| **Р8** | Эзотерические протоколы | Типы эзотерических протоколов. Методы построения и анализа криптографических протоколов. |

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

| Направление воспитательной | Вид воспитательной | Технология воспитательной | Компетенция | Результаты обучения |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| деятельности | деятельности | деятельности | | |
| Профессиональное воспитание | учебно-исследовательская, научно-исследовательская | Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности | ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | З-7 - Описывать криптографические протоколы, применяемые в компьютерных сетях |

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Криптографические протоколы**

**Электронные ресурсы (издания)**

**Печатные издания**

1. Фергюсон, Фергюсон Н., Шнайер, Шнайер Б., Селина, Н. Н., Журавлев, А. В.; Практическая криптография; Диалектика, Москва ; Санкт-Петербург ; Киев; 2005 (17 экз.)

2. , Ященко, В. В.; Введение в криптографию : Учебник.; МЦНМО : Питер, СПб.; Москва; Харьков; Минск; 2001 (11 экз.)

3. Черемушкин, А. В.; Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для студентов вузов, обучающихся по специальности "Компьютерная безопасность".; Академия, Москва; 2009 (6 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**

Общероссийский математический портал http://www.mathnet.ru/

Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/

Сайт издательства Elsevier http://www.sciencedirect.com/

Сайт кафедры: http://kma.imkn.urfu.ru

Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index

Сайт библиотеки университета http://lib.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 | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 2 | Практические занятия | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 3 | Консультации | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | **Не требуется** |
| 4 | Текущий контроль и промежуточная аттестация | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | **Не требуется** |
| 5 | Самостоятельная работа студентов | Мебель аудиторная с количеством рабочих мест в | Office Professional 2003 Win32 Russian CD-ROM |

| | | | |
|---|---|---|---|
| | | соответствии с количеством студентов<br>Подключение к сети Интернет | Свободное ПО:Google Crome |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
**Основы построения защищённых компьютерных сетей**

Рабочая программа дисциплины составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Бакланов Валентин Викторович | кандидат технических наук, доцент | Доцент | Департамент радиоэлектроники и связи |
| 2 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

**Рекомендовано учебно-методическим советом института** Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

## 1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**Авторы:**

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **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 |
|---|---|---|
| **Р1** | Методология оценки безопасности информационных технологий | Основные подходы к проектированию защищенных телекоммуникационных систем. Структура ГОСТ Р ИСО/МЭК 15408. Методология оценки безопасности информационных технологий. Контекст безопасности. Подход общих критериев. Понятия безопасности. Описательные возможности общих критериев. Виды оценок. Поддержка доверия. Виды требований безопасности (функциональные и доверия). Профиль защиты.<br>Профиль защиты «Клиентская операционная система». Среда безопасности. Цели безопасности. Функциональные требования. Требования доверия. Описание объекта оценки. Среда безопасности объекта оценки. Требования безопасности информационных технологий. Функции безопасности объекта оценки. Логическое обоснование целей и требований безопасности. |
| **Р2** | Проектирование подсистем защиты информации от несанкционированного доступа | Функциональная схема комплексной системы защиты информации. Модель управления доступом к защищаемым ресурсам.<br>Проектирование подсистем идентификации и аутентификации на основе носителей ключевой информации. |

| | | |
|---|---|---|
| | | Общие принципы реализации механизмов разграничения прав доступа. Практическая реализация подсистемы управления доступа к каталогам. Состав и реализация диспетчера доступа к ресурсам. Непротиворечивые правила назначения (изменения) прав доступа. Формальная модель диспетчера доступа. Функциональная схема системы защиты, реализующая механизм уровневого контроля списков санкционированных событий. Алгоритм контроля доступа пользователя к ресурсам защищаемого объекта.<br><br>Реализация механизма обеспечения замкнутости программной среды. Механизмы контроля целостности информации и их реализация. Механизмы аудита событий и их реализация.<br><br>Технология доверенной загрузки операционной системы. Структура программно-аппаратного комплекса защиты загрузки операционной системы. Разработка программного компонента идентификации и аутентификации пользователей, функционирующего до загрузки операционной системы. Структура программы начальной загрузки. Программирование загрузчика персонального компьютера. Применение технологии виртуальных машин для тестирования разрабатываемого компонента идентификации и аутентификации. |
| **Р3** | Проектирование подсистем криптографической защиты информации | Разработка интерфейсной части системы криптографической защиты информации на основе библиотек, предоставляемых криптопровайдером. Реализация функций шифрования, подписывания и проверки электронно-цифровой подписи с использованием алгоритмов RSA, ГОСТ Р34.10-94 и ГОСТ 28147-89.<br><br>Порядок взаимодействия приложений с криптографическими модулями операционной системы на базе Microsoft Cryptographic Application Programming Interface (MS Crypto API).<br><br>Особенности проектирования интерфейса пользователя для генерации ключевой информации на основе клавиатурного ввода, записи и извлечения ключей на носители, гарантированного уничтожения файлов. Реализация функций шифрования (зашифрования, расшифрования, подписывания, проверки подписи) файлов по выбору в компилирующей визуальной среде разработки прикладных программ Delphi. Реализация Windows-подобного интерфейса пользователя для генерации ключевой информации на основе клавиатурного ввода, записи ключа на ключевой носитель. Разработка руководства пользователя программы криптографической защиты информации.<br><br>Разработка системы защищенного документооборота на базе программно-аппаратного комплекса, реализующего подсистему криптографической защиты информации. Архитектура системы защищенного документооборота. Структура и функции удостоверяющего центра. Установка и конфигурация компонентов удостоверяющего центра. Выпуск |

| | | |
|---|---|---|
| | | сертификатов пользователей. Настройка клиентов системы защищенного документооборота. |
| **Р4** | Проектирование подсистем обнаружения компьютерных атак | Технология интеллектуальных многоагентных систем. Понятие агентов защиты. Архитектура многоагентных систем. Агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений. Спецификация «системного ядра» многоагентной системы. Проектирование компонентов многоагентной СОА. Разработка сенсоров различного типа. Протоколы информирования о событиях, зафиксированных сенсором.<br>Методологии обнаружения атак: простой поиск по шаблону, поиск по шаблону с сохранением состояния, разбор протоколов, эвристический анализ, обнаружение аномалий, анализ соответствия политике безопасности. Основные математические методы, лежащие в основе обнаружения аномалий, и их реализации в СОА.<br>Модель системы корреляции событий информационной безопасности |
| **Р5** | Проектирование защищенных автоматизированных информационных систем | Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.<br>Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах |
| **Р6** | Проектирование средств защиты информации от несанкционированного распространения | Общие принципы построения подсистем защиты от несанкционированного распространения программного обеспечения на основе электронных ключей Guardant<br>Использование электронных ключей Guardant для защиты приложений |

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-исследовательск | Технология формирования уверенности и готовности к | ПК-4 - Способен проводить инструментальный мониторинг | У-3 - Применять методы анализа защищенности компьютерных |

| | | | | |
|---|---|---|---|---|
| | ая | самостоятельной успешной профессиональной деятельности | защищенности компьютерных систем и сетей | систем и сетей |

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Основы построения защищённых 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. 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.)

2. Платонов, В. В.; Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность".; Академия, Москва; 2013 (5 экз.)

3. 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.)

**Профессиональные базы данных, информационно-справочные системы**

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

2. Бакланов В. В. Программно-аппаратная защита информации / Бакланов В.В., Ваулин С.С., Синадский Н.И. — УМК. — 2007. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7232>.

3. Гайдамакин Н.А. Учебно-методический комплекс дисциплины "Основы создания и эксплуатации защищенных компьютерных систем" [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (8,17 Мб) .— Екатеринбург : [б. и.], 2007 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1374>.

4. Бакланов В.В. Основы проектирования защищенных телекоммуникационных систем / Бакланов В.В. — УМК. — 2007. Материалы подготовлены в АИС

"Управление учебным процессом". — в корпоративной сети УрФУ. —

<URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7115>.

**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**

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

## 3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Основы построения защищённых 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<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 2 | Лабораторные занятия | Мебель аудиторная с количеством рабочих мест в | Office Professional 2003 Win32 Russian CD-ROM |

| | | | |
|---|---|---|---|
| | | соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Свободное ПО:Google Crome |
| 3 | Консультации | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | **Не требуется** |
| 4 | Текущий контроль и промежуточная аттестация | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | **Не требуется** |
| 5 | Самостоятельная работа студентов | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
**Программно-аппаратные средства**
**обеспечения информационной безопасности**

Рабочая программа дисциплины составлена авторами:

| № п/п | Фамилия Имя Отчество | Ученая степень, ученое звание | Должность | Подразделение |
|---|---|---|---|---|
| 1 | Бакланов Валентин Викторович | кандидат технических наук, доцент | Доцент | Департамент радиоэлектроники и связи |
| 2 | Синадский Николай Игоревич | кандидат технических наук, Доцент | Доцент | УНЦ "Информационная безопасность" |

**Рекомендовано учебно-методическим советом института** Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

## 1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

**Авторы:**

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **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 |
|---|---|---|
| **Р1** | Технология межсетевого экранирования | Стратегии и средства межсетевого экранирования.<br>Создание защищенных сегментов при работе в сети<br>Интернет с использованием межсетевых экранов. Требования руководящих документов к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.<br>Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS.<br>Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого. |
| **Р2** | Организация виртуальных частных сетей | Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и |

| | | |
|---|---|---|
| | | настройка VPN. Анализ защищенности передаваемой информации.<br><br>Защита данных на сетевом уровне. Протокол SKIP.<br><br>Протокол IPSec. Организация VPN средствами СЗИ «VipNet», «Игла», «Верба», «StrongNet». Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.<br><br>Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server. Генерация сертификата открытого ключа для web-сервера.<br><br>Настройка SSL-соединения.<br><br>Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP.<br><br>Защищенный обмен электронной почтой. |
| **Р3** | Функции, выполняемые программно-аппаратными средствами защиты<br><br>компьютерной информации<br><br>(СЗИ). Применение средств криптографической защиты информации | Требования к специализированным средствам защиты информации от несанкционированного доступа. Алгоритм работы СЗИ, предназначенного для обработки информации ограниченного доступа. Механизмы организации контроля доступа до загрузки ОС.<br><br>Взаимодействие СЗИ с BIOS системной платы. Контроль целостности системного программного обеспечения и аппаратных средств. Программно-аппаратная идентификация и аутентификация пользователей. Возможности СЗИ по криптографическому преобразованию информации. Шифрование «по требованию», прозрачное шифрование с организацией виртуальных логических дисков. Способы формирования ключевой информации. Контроль и удаление<br><br>«технологического мусора». Формирование и поддержка изолированной программной среды. Реализация дискреционной и мандатной моделей разграничения доступа. Обзор современных отечественных средств защиты информации. Основные характеристики системы криптографической защиты информации (СКЗИ) «Верба».<br><br>Инициализация СКЗИ «Верба» на рабочей станции. Генерация, импорт и экспорт ключей. Шифрование и обмен шифрованной информацией.<br><br>Применение системы криптографической защиты конфиденциальной информации на примере СКЗИ «StrongDisk», «Secret Disk». Основные характеристики СКЗИ. Инициализация системы. Создание и работа с защищенными логическими дисками. Работа с защищенными дисками. Настройка параметров СКЗИ. Управление секретными дисками. Хранение конфиденциальной информации на съемных носителях. |

| | | |
|---|---|---|
| **Р4** | Применение СЗИ от НСД для организации защищенных компьютерных систем. Применение аппаратных модулей доверенной загрузки | Назначение и возможности СЗИ от НСД, требования, предъявляемые к ним. Использование специализированных аппаратно-программных средств защиты информации от НСД на примере программноаппаратных комплексов «Страж-NT», «Dallas Lock», «Secret Net». Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Организация учета сменных носителей информации. Регистрация событий. Гарантированное удаление данных. Настройка механизма шифрования данных. Назначение и возможности аппаратных модулей доверенной загрузки на примере комплексов АккордАМДЗ и электронный замок «Соболь». Регистрация пользователей и назначение им персональных идентификаторов и паролей для входа в систему. Управление параметрами процедуры идентификации пользователя. Регистрация событий, имеющих отношение к безопасности системы. Контроль целостности файлов на жестком диске и физических секторов жесткого диска. Защита от несанкционированной загрузки операционной системы со съемных носителей. |
| **Р5** | Технологии защищенной обработки информации | Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory. |
| **Р6** | Обеспечение безопасности АСУ ТП | Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Уровни АСУ ТП. Уязвимости АСУ ТП. |

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-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | У-2 - Применять инструментальные средства проведения мониторинга защищенности компьютерных систем |

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Программно-аппаратные средства обеспечения 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. 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. Платонов, В. В.; Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность".; Академия, Москва; 2013 (5 экз.)

3. 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.)

**Профессиональные базы данных, информационно-справочные системы**

1. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008 .— в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

2. Бакланов В. В. Программно-аппаратная защита информации / Бакланов В.В., Ваулин С.С., Синадский Н.И. — УМК. — 2007. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7232>.

**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**

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

## 3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Программно-аппаратные средства обеспечения 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<br>Рабочее место преподавателя<br>Доска аудиторная<br>Периферийное устройство<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 2 | Практические занятия | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |
| 3 | Консультации | Мебель аудиторная с количеством рабочих мест в | **Не требуется** |

| | | | |
|---|---|---|---|
| | | соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | |
| 4 | Текущий контроль и промежуточная аттестация | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Рабочее место преподавателя<br>Доска аудиторная | **Не требуется** |
| 5 | Самостоятельная работа студентов | Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов<br>Персональные компьютеры по количеству обучающихся<br>Подключение к сети Интернет | Office Professional 2003 Win32 Russian CD-ROM<br>Свободное ПО:Google Crome |