Аннотация к рабочей программе дисциплины
Администрирование операционных систем
Специальность: 10.05.03. Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем форма обучения
очная

**Объем дисциплины (модуля):** 8 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (5 семестр), экзамен (6 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Администрирование операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Администрирование операционных систем» является изложение основополагающих принципов администрирования операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Администрирование операционных систем»:

- дать представление об основных задачах администрирования ОС и методах их решения;
- научить использовать встроенные средства ОС для решения задач администрирования ОС.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

В результате изучения дисциплины студент должен:

знать:

- основные задачи и функции администратора ОС;
- знать типы, версии и редакции ОС Windows, Linux, Unix;
- основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности;
- знать основные команды, применяемые при администрировании ОС Windows, Linux, Unix;
- основы разработки сценариев;
- базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных;
- основные электронные ресурсы по теме безопасного администрирования ОС.

уметь:

- выполнять установку и конфигурирование ОС Windows, Linux, Unix;
- выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix;
- выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix;
- выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix;
- конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix;

- выполнять резервное копирование и восстановление данных в ОС Windows, Linux, Unix;



- конфигурировать и обслуживать основные сервисы безопасности ОС;
- определять ресурсы, подлежащие защите;
- работать с технической литературой и специализированными электронными ресурсами.

владеть:

- навыками базового администрирования ОС Windows, Linux, Unix;
- навыками работы в командной строке;
- навыками написания и выполнение административных сценариев;  навыками поска технической информации.

**Краткое содержание дисциплины (модуля)** Тема
1. Введение в администрирование ОС.
Тема 2. Базовые инструменты администрирования ОС Windows.
Тема 3.Управление локальными пользователями в ОС Windows.
Тема 4. Управление дисковыми ресурсами.
Тема 5. Сетевые параметры в ОС Windows.
Тема 6. Система доменных имен.
Тема 7. Протокол динамической конфигурации хоста.
Тема 8. Настройка файлового сервера под управлением ОС Windows.
Тема 9. Администрирование доменов в сетях Windows.
Тема 10. Настройка удаленного доступа в Windows.
Тема 11. Резервное копирование данных.
Тема 12. Мониторинг работы и контроль производительности ОС Windows.
Тема 13. Автоматизация задач администрирования в ОС Windows. PowerShell.
Тема 14. Общий обзор Unix-like систем. ОС FreeBSD.
Тема 15. Командная строка FreeBSD.
Тема 16. Управление локальными пользователями в ОС FreeBSD.
Тема 17. Управление дисковыми ресурсами, ФС UFS.
Тема 18. Ограничение доступа к фалам и каталогам.
Тема 19. Сетевые параметры в ОС FreeBSD.
Тема 20. Загрузка ОС FreeBSD.  Сборка ядра, обновление системы.
Тема 21. Установка программного обеспечения в ОС FreeBSD.
Тема 22. Сервер имен под управлением ОС FreeBSD.
Тема 23. DHCP-сервера под управлением ОС FreeBSD.
Тема 24. Файловый сервер под управлением ОС FreeBSD.
Тема 25. Организация удаленного доступа к серверу под управлением ОС FreeBSD.
Тема 26. Организация резервного копирования и восстановления данных в ОС FreeBSD.
Тема 27. Мониторинг работы и контроль производительности ОС FreeBSD.
Тема 28. Обеспечение отказоустойчивости ОС FreeBSD.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

## АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (9 семестр)

**Планируемые результаты освоения:**

ОПК-5.1

Перечень планируемых результатов обучения по дисциплине (модулю):

Знать:

1) Основные определения и термины из области анализа и оценки рисков информационной безопасности;
2) Методики анализа и оценки рисков информационной безопасности;
3) Принципы построения и сопровождения системы управления информационными рисками и системы управления информационной безопасностью.

Уметь:

1) Определять субъекты и объекты информационной системы;
2) Составлять модель угроз и модель злоумышленника;
3) Разрабатывать политику информационной безопасности;
4) Анализировать и оценивать риски информационной безопасности;
5) Внедрять и сопровождать систему управления информационными рисками и систему управления информационной безопасностью.

Владеть:

1) Навыками разработки документации стратегического и тактического уровней;
2) Инструментами реализации системы управления информационными рисками и системы управления информационной безопасностью;
3) Навыками расчёта величины риска информационной безопасности.

Аннотация к рабочей программе дисциплины

**Большие данные**

Специальность: 10.05.03. Информационная безопасность автоматизированных систем.

Специализация: Безопасность открытых информационных систем

Уровень высшего образования: специалитет форма обучения

очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачёт (9 семестр).

**Планируемые результаты освоения:** ОПК-8

В результате освоения дисциплины студент должен:

**знать:**

- принципы и методы хранения и обработки данных большого объема;
- основы администрирования систем хранения и обработки больших данных;
- теоретические основы анализа данных;
- технологии, используемые в современных системах хранения и обработки больших данных;
- особенности защиты информации в системах хранения и обработки больших данных;

**уметь:**

- обосновать выбор стека технологий для хранения и обработки данных большого объема;
- администрировать системы хранения и обработки больших данных;
- использовать технологии для анализа данных большого объема;
- оптимизировать выполнение задач над данными большого объема;
- применять инструментарий обеспечения информационной безопасности в системах хранения и обработки больших данных.

**Цели и задачи освоения дисциплины:**

Цель: приобретение знаний и умений в области технологий хранения, обработки и защиты информации в системах больших данных.

Задачи:

-обеспечить освоение основных принципов работы с данными в парадигме Big Data; -ознакомить обучающихся с доступным стеком технологий в области хранения и обработки больших данных;

-научить обучающихся пользоваться инструментарием системы хранения и обработки больших данных на примере фреймворка Apache Hadoop;

-развить навыки обеспечения безопасности информации в системах хранения и обработки больших данных.

**Краткое содержание дисциплины:**

Дисциплина включает 8 разделов:

1. Большие данные. Принципы и технологии. NoSQL решения.
2. Фреймворк Apache Hadoop. Основы.
3. Введение в анализ данных.
4. Информационная безопасность Apache Hadoop.
5. Фреймворк Apache Hadoop. Продвинутый уровень.
6. Фреймворк Apache Hadoop. Системы управления базами данных.
7. Фреймворк Apache Hadoop. Альтернативные инструменты анализа данных.
8. Фреймворк Apache Spark.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Дополнительные главы математики для обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (5 семестр)

**Планируемые результаты освоения:**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности
Знать

- совокупности математических методов

Уметь

- разрабатывать, обосновывать и реализовывать процедуры решения задач

профессиональной деятельности;

- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть

- необходимыми математическими методами для решения задач профессиональной деятельности.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Дополнительные главы математической статистики
Рабочая программа для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (6 семестр)

**Планируемые результаты освоения:**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности

Знать

- совокупности математических методов

Уметь

- разрабатывать, обосновывать и реализовывать процедуры решения задач

профессиональной деятельности;

- способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

Владеть

- необходимыми математическими методами для решения задач профессиональной деятельности.

Аннотация к рабочей программе дисциплины
Защита в операционных системах
Специальность: 10.05.03. Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем форма обучения
очная

**Объем дисциплины (модуля):** 8 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (7 семестр), экзамен (8 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Защита в операционных системах» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Защита в операционных системах» является изложение основополагающих принципов защиты операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Защита в операционных системах»:

- дать представление об основных угрозах ИБ для современных ОС;
- научить оценивать уровень защищенности ОС с учетом актуальных моделей угроз и требований руководящих документов;
- дать основы системного подхода к обеспечению безопасности в современных ОС;
- изучить сервисы безопасности современных ОС и научить использовать их для защиты ОС.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

В результате изучения дисциплины студент должен:

знать:

- основные понятия и положения защиты информации в ОС;
- основные угрозы ИБ в ОС;
- ресурсы, подлежащтие защите;
- основные понятия программно-технического уровня ИБ;
- требования к обеспечению ИБ в ОС;
- основные сервисы безопасности ОС, принципы их организации и структуру;
- методы обеспечения ИБ в ОС;
- перечень программно-технических мер ИБ в ОС;
- основные ресурсы для поиска информации об уязвимостоях ОС;
- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;

уметь:

- проводить анализ угроз информационной безопасности в ОС;
- проводить классификацию возможных угроз ИБ в ОС;
- оценивать эффективность и надежность защиты ОС;

- находить информацию об актуальных угрозах ОС, уязвимостях ОС;



- выявлять слабые места в защите ОС;
- конфигурировать встроенные сервисы безопасности ОС;
- проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- проводить инструментальный контроль защищенности ОС;
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;

владеть:

- навыками поиска и анализа информации об уязвимостоях ОС;
- навыками анализ угроз информационной безопасности в ОС;
- навыками безопасного администрирования ОС;
- навыками оценки уровня безопасности ОС;
- навыками использования средств инструментального контроля защищенности ОС.

**Краткое содержание дисциплины (модуля)**

Тема 1. Основные понятия и положения защиты информации в АС.
Тема 2. Угрозы ИБ: определения, анализ и классификация.
Тема 3. Основные направления и методы реализации угроз ИБ.
Тема 4. Программно-технические меры ИБ, сервисы ИБ.
Тема 5. Требования безопасности информации к операционным системам Тема
6. Модели безопасности основных операционных систем.
Тема 7. Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 8. Дополнительные механизмы защиты в ОС Windows.
Тема 9. Организация защищенного удаленного доступа в ОС Windows.
Тема 10. Сетевая безопасность в ОС Windows.
Тема 11. Аудит безопасности в ОС Windows.
Тема 12. Базовые сервисы безопасности в Unix-like систем. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 13. Дополнительны механизмы защиты объектов ФС в Unix-like системах.
Тема 14. Шифрование, контроль целостности в Unix-like системах.
Тема 15. Мандатная модель управления доступом в Unix-like системах.
Тема 16. Подключаемые модули аутентификации.
Тема 17. Организация защищенного удаленного доступа в Unix-like системах.
Тема 18. Сетевая безопасность в Unix-like системах.
Тема 19. Аудит безопасности в Unix-like системах.
Тема 20. Общие рекомендации по защите ОС.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Защита государственных информационных систем и персональных данных»
Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

форма обучения очная

**Объем дисциплины (модуля):** 4 зачетных единиц, 144 академических часа.

**Форма промежуточной аттестации:** экзамен (9 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Безопасность персональных данных» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Программа дисциплины «Безопасность персональных данных» ориентирована на достижение следующих целей:

- получения знаний о принципах обработки персональных данных в РФ;
- освоение методов и способов построения системы защиты персональных данных.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить основные нормативно-правовые акты в области защиты персональных данных и области их применения;
- изучить алгоритмы классификации информационных систем персональных данных;
- научить обучающихся строить модели нарушителя и угроз безопасности информации;
- сформировать у обучающегося навыки правильного обоснованного выбора мер по защите информации и аргументированно исключать не подходящие
- научить обучающихся разрабатывать проект системы защиты информации, обрабатываемой в информационных системах персональных данных.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-17: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма

В результате изучения дисциплины студент должен:

знать:

- нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных, их содержание, предмет регулирования и сферу применения;
- основные понятия, термины и определения в области обработки и защиты персональных данных;
- отечественные нормативно-правовые акты, методические документы и стандарты в области защиты информации и защиты персональных данных;
- существующие базы знаний и информационные системы нормативных правовых актов РФ;

- правовые основания обработки персональных данных;



- необходимые параметры и характеристики информационной системы персональных данных, необходимые для определения требуемого уровня защищенности персональных данных;
- основные угрозы безопасности персональных данных;
- состав и принципы написания организационно-распорядительной документации по защите информации;
- способы использования и обозначения требований по защите информации в организационно-распорядительной документации;
- правила разработки технического задания на создание АС в защищенном исполнении;
- правила разработки технического проекта на создание системы защиты персональных данных;
- необходимые для написания документов НПА и ГОСТы;
- нормативные и методические документы ФСТЭК России и ФСБ России по моделированию нарушителя и угроз безопасности информации;
- методику определения угроз безопасности персональных данных в соответствии с требованиями законодательства РФ;
- отечественные нормативно-правовые акты и методические документы в области защиты информации и защиты персональных данных, описывающие требования и меры по защите персональных данных;
- методику формирования набора организационных и технических мер по защите информации;
- основные классы и характеристики средств защиты информации;
- правила подбора средств защиты информации для обеспечения необходимого уровня защищенности персональных данных.

уметь:

- применять нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных для конкретных задач и ситуаций в области защиты информации;
- использовать средства поиска информации в сети Интернет;
- использовать специальные информационные системы, базы знаний и электронные библиотеки для поиска и работы с нормативными правовыми документами;
- осуществлять подбор и анализ нормативных правовых документов и информации необходимых для решения конкретных задач по обработке и защите персональных данных;
- определять тип обрабатываемых персональных данных и правовые основания их обработки и хранения;
- определять уровень защищенности персональных данных при их обработке в информационных системах персональных данных;
- построить модель нарушителя и модель угроз информационной безопасности персональных данных;
- разрабатывать проекты организационно-распорядительной документации по защите персональных данных;
- разрабатывать проекты документов Техническое задание и Технический проект на создание системы защиты персональных данных;

- построить модель нарушителя и модель угроз информационной безопасности персональных данных;
- формировать набор требований по обеспечению безопасности персональных данных;



- формировать набор и определять состав организационных и технических мер по защите персональных данных;
- осуществлять подбор средств защиты информации;
- определять состав контрольных и периодических мероприятий по поддержке реализованной в системе защите персональных данных политики безопасности.

**Краткое содержание дисциплины (модуля)**

Тема 1. Законодательство по защите персональных данных

Тема 2. Информационные системы персональных данных

Тема 3. Обследование информационных систем

Тема 4. Модель нарушителя безопасности персональных данных

Тема 5. Модель угроз безопасности персональных данных

Тема 6. Определение состава требований и мер по защите персональных данных Тема 7. Мероприятия по защите персональных данных

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

10.05.03. Информационная безопасность автоматизированных систем специализация «Безопасность открытых информационных систем» форма обучения очная **Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** экзамен (7 семестр)

**Планируемые результаты освоения:**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности

знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ

России, ФСТЭК России в данной области;

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; уметь:
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации; владеть:
- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и контроля показателей технической защиты

информации;

- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Защита корпоративных сетей для обучающихся по направлению подготовки (специальности)
10.05.03 Информационная безопасность автоматизированных систем
Профиль: Безопасность открытых информационных систем форма обучения очная
Специалитет

**Объем дисциплины:** 8 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (7 семестр), экзамен (8 семестр).

**Планируемые результаты освоения:** ОПК-12, 13

В результате изучения дисциплины студент должен:

Знать:

- основы проектирования и работы безопасных коммутируемых сетей;
- организацию и распространение виртуальные локальные сети;
- основы безопасной маршрутизации между сегментами внутри кампусной сети;
- основы безопасности коммутируемых сетей на уровне распределения (distribution);
- основы безопасности коммутируемых сетей на уровне доступа (access);

Уметь:

- настраивать порты коммутатора для подключения WI-FI-точек доступа;
- проектировать и настраивать маршрутизацию между VLAN;
- управлять беспроводным котроллером;
- конфигурировать протоколы FHRP;
- настраивать протоколы класса Spanning Tree;
- применять технологии отказоустойчивости, высокой доступности и мониторинга безопасности компьютерных сетей.

Аннотация к рабочей программе дисциплины

**Криптографические протоколы**

Специальность:10.05.03 Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем форма обучения очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачёт (8 семестр).

**Планируемые результаты освоения: ОПК-10**

Знать:

- основные типы криптографических протоколов и их свойства;
- криптографические стандарты;
- типовые криптографические протоколы и основные требования к ним;
- основные схемы цифровой подписи;
- протоколы идентификации;
- протоколы передачи и распределения ключей;

уметь:

- использовать симметричные и асимметричные шифры системы для построения криптографических протоколов;
- формулировать свойства безопасности криптографических протоколов;
- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

владеть:

- криптографической терминологией;
- навыками программной реализации криптографических протоколов;
- навыками оценки эффективности протокола;
- способностью читать и понимать научную и инженерно-техническую литературу по криптографическим протоколам, в том числе на английском языке;
- простейшими подходами к анализу безопасности криптографических протоколов.

**Цели и задачи освоения дисциплины:** В дисциплине изучаются основные виды базовых и прикладных протоколов, таких как цифровые подписи общего и специального назначения, электронная жеребьевка, разделение секрета, покер по телефону, электронные выборы, электронные деньги, конфиденциальные вычисления, идентификация и аутентификация, управление ключами.

В качестве прикладных протоколов рассматриваются семейства IPSec и SSL. Рассматриваются вопросы полноты и корректности протоколов, доказательства их свойств безопасности.

**Краткое содержание дисциплины:**

Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы. Полнота и корректность. Цифровые подписи общего назначения. Математическая модель. Атаки и угрозы. Цифровые подписи RSA и Рабина. Цифровая подпись Эль-Гамаля и связанные с ней схемы. Стандарты DSA и ГОСТ Р 34.10-94. Эллиптическая кривая над полем вещественных чисел и над полем GF(p). Задача дискретного логарифмирования на эллиптической кривой. Подпись Эль-Гамаля на эллиптической кривой. Стандарты ECDSA и ГОСТ Р 34.10-2012. Цифровые подписи специального назначения. Коллективная подпись. Неотрицаемая подпись. Слепая подпись. Подписи со скрытым каналом. Протоколы подбрасывания монеты. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью. Пример протокола с безусловной секретностью. Протоколы привязки к биту. Понятие о разделении секрета. Совершенность и идеальность СРС. Пороговые схемы разделения секрета. Схема Шамира, схема Блэкли, СРС на основе Китайской теоремы об остатках. СРС для произвольной структуры доступа. Протоколы конфиденциальных вычислений. Задача миллионеров и протокол Яо. Логический контур. Протокол GMW. Протоколы идентификации. Классификация. Требования. Парольные схемы. Разновидности. Область применения. Схемы рукопожатия. Интерактивные системы доказательств. Пример интерактивной системы доказательств для языка «Квадратичные невычеты». Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов». Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схемы Фиата-Шамира, Файге-Фиата-Шамира, Шнорра. Их полнота и корректность. Схема идентификации Окамото и теорема о ее условной стойкости. Схема Гиллу-Кискатр. Ее полнота и корректность. Протокол «Покер по телефону». Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема Шаума. Протоколы голосования. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-Mouth Frog, Yahalom. Их анализ. Протокол Нидхема-Шредера. Его анализ. Протокол Отвея-Рииса. Его анализ. Бесключевой протокол Шамира, протокол ДиффиХэллмана и атака «Человек посередине». Противодействие этой атаке. Протокол НидхемаШредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Стандарт x.509. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

## МЕТОДЫ И СРЕДСТВА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (10 семестр)

**Планируемые результаты освоения:**

ОПК-8

Перечень планируемых результатов обучения по дисциплине (модулю):

**Знать:**
1) Основные направления применения искусственного интеллекта в информационной безопасности;
2) Типы задач машинного обучения;
3) Основные алгоритмы моделей машинного обучения.

**Уметь:**
1) Выбирать модели МО для решения задач ИБ;
2) Применять программные инструменты и библиотеки для решения задач ИБ с помощью методов МО;
3) Формировать датасеты для обучения моделей МО; 4) Оценивать качество моделей МО.

**Владеть:**
1) Навыками построения и обучения моделей МО на языке Python с использованием библиотек NumPy, Keras, Tensorflow, Scikit-learn и др.
2) Навыками формирования датасетов для машинного обучения (разметка текстов, нормализация, стемминг, кодирование и пр.)
3) Навыками оценки качества моделей машинного обучения с помощью метрик (матрицы ошибок (confusion matrix), accuracy, precision, recall, F-меры, AUC-ROC и др.).

Аннотация к рабочей программе дисциплины

**Методы и средства криптографической защиты информации**

Специальность:10.05.03 Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем форма обучения очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачёт (8 семестр).

**Планируемые результаты освоения: ОПК-3, ОПК-10**

знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов;
- криптографические стандарты;
- использование криптографических стандартах в информационных системах;
- о системах криптографической защиты информации (СКЗИ).

уметь:

- применять криптографические алгоритмы на практике;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- осуществлять программную реализацию криптографических алгоритмов;
- пользоваться научно-технической литературой в области криптографии;

владеть:

- криптографической терминологией;
- навыками программной реализации криптографических алгоритмов;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии;
- средствами обеспечения информационной безопасности;
- навыками определения видов и форм информации, подверженных угрозам и возможных методов и путей устранения этих угроз.

**Цели и задачи освоения дисциплины:** В курсе изучаются исторические основы криптографии и криптоанализа, основы современой симметричной и асимметричной криптографии, основные криптографические примитивы такие как симметричные шифры: SPсети, сети Файстеля (на примере ГОСТ Р 34.12-2015 "Магма"), XLPS-шифры (SQUARE, AES, ГОСТ Р 34.12-2015 "Кузнечик"), режимы блочных шифров, соответствующие стандарты FIPS и ГОСТ Р 34.13-2015, поточные симметричные шифры, теория секретности Шеннона, теория имитостойкости Симмонса, защитные контрольные суммы и хэш-функции,стандарты

SHA-1, SHA-3, ГОСТ Р 34.10-94, ГОСТ Р 34.11-2012, коды аутентификации, асимметричные криптосистемы (RSA, Рабина, Эль-Гамаля, Диффи-Хэллмана, Шамира).

**Краткое содержание дисциплины:**

Основные понятия и определения криптографии. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. История криптографии. Основные этапы становления науки криптографии. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу. Композиции шифров. Enigma. Шифр Хейглина. Математическая модель шифра. Атаки и угрозы шифрам. Блочные шифры и их ключевая система. Замены и перестановки. S-P-сеть. Сеть Файстеля. Шифр ГОСТ Р 34.12-2015 "Магма". Конечные кольца и поля многочленов. XLPS-шифры. Шифры SQUARE, AES, ГОСТ Р 34.12-2015 "Кузнечик". Режимы шифрования. ГОСТ Р 34.13-2015. Многократное шифрование. Композиция блочных шифров. Теория секретности Шеннона. Совершенные шифры. Энтропийные характеристики шифров. Идеальные шифры. Избыточность языка. Ложные ключи и расстояние единственности. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры. Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. Нелинейные регистры сдвига. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость. Защитные контрольные суммы. Криптографические хэш-функции и требования к ним. Подходы к проектированию хэш-функций. Схема Меркла-Дамгарда. Хэш-функции на основе блочного шифра. Атака дописыванием в схеме Меркла-Дамгарда и способы противостояния ей. Хэш-функция ГОСТ Р 34.11-2012. Хэш-функции SHA-1 и SHA-2. Схема «губка» и SHA-3. Коды аутентификации сообщений. HMAC. Асимметричные шифры. RSA, Рабина, Эль-Гамаля. Цифровые подписи. DSA и ГОСТ Р 34.10-94. Проблема дискретного логарифмирования на эллиптической кривой. Подписи на эллиптической кривой. Стандарты ECDSA и ГОСТ Р 34.10-2012.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ
для обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (6 семестр)

**Планируемые результаты освоения:**

ОПК-5.1

Перечень планируемых результатов обучения по дисциплине (модулю):
Знать:

- основные модели доступа в информационной системе;
- методы формального описания модели злоумышленника;
- основные способы формального описания и анализа политик безопасности;
- методы анализа модели угроз.

Уметь:

- реализовывать основные модели доступа в информационной системе;
- формально описывать модель злоумышленника;
- формально описывать и анализировать политику безопасности;
- анализировать модель угроз.

Владеть:

- навыками реализации основных моделей доступа в информационной системе;
- навыками формального описания модели злоумышленника; • навыками формального описания и анализа политик безопасности;
- навыками анализа модели угроз.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Научно-проектный (исследовательский) семинар»
10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

**Объем дисциплины (модуля):** 8 зачетных единиц, 288 академических часов.

**Форма промежуточной аттестации:** Дифференцированный зачет (7,11 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Основной целью дисциплины является развитие навыков студента для проведения самостоятельной научно-исследовательской работы.

Задачи дисциплины– дать основы:

- развить навыки поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;
- научить правилам оформления списка литературных источников;
- навыками проведения научно-исследовательской работы и применения методов научных исследований в профессиональной деятельности;
- развить навыки разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ;
- дать опыт публичной защиты собственного научного труда.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

УК-2. Способен управлять проектом на всех этапах его жизненного цикла.

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни.

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

В результате изучения дисциплины студент должен: знать:

- правила оформления отчета по курсовой работе;
- правила оформления списка литературы; • основные научные проблемы в области ИБ; уметь:
- применять методы научных исследований в профессиональной деятельности;

- осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности; владеть:
- навыками проведения научно-исследовательской работы;
- навыками разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ.

**Краткое содержание дисциплины (модуля)**

1. Актуальные проблемы и научно-исследовательские задачи в области ИБ
2. Презентация и обсуждение тем проектов
3. Поиск и систематизация научной информации. Работа с литературой.
4. Представление и обсуждение литературного обзора по теме проекта
5. Подготовка научно-технического отчета
6. Презентация и обсуждение плана реализации проекта
7. Правила презентации научного исследования
8. Презентация и обсуждение промежуточных результатов реализации проекта
9. Презентация и обсуждение результатов реализации проекта

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ 10.05.03. Информационная безопасность автоматизированных систем специализация «Безопасность открытых информационных систем» форма обучения очная

**Объем дисциплины (модуля):** 4 зачетных единиц.

**Форма промежуточной аттестации:** дифференцированный зачет.

**Цели и задачи освоения дисциплины (модуля)**

Целью дисциплины «Обеспечение защищенности объектов критической информационной инфраструктуры» является обучение студентов основам проектирования защищенных автоматизированных систем, ознакомление с оборудованием и организации защиты датчиков, автоматизированных узлов и диспетчерских.

Задачи дисциплины «Обеспечение защищенности объектов критической информационной инфраструктуры»:

- изучить современные технологические процессы и их технологию;
- основную нормативно-техническую документацию;
- изучить виды оборудования и принципы работы;
- изучить всевозможные угрозы, влияющие на работу оборудования и технологического процесса в целом;
- научиться строить модели нарушителя для предложенной технологической линейки или технологии;
- научиться настраивать оборудование;
- научиться строить принципиальные и подробные электрические схемы, в том числе с использованием эмуляторов и имитационных тренажеров;
- научиться разрабатывать мнемосхемы и скада системы для предложенного технологического процесса.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-6 – Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

**Обеспечение защищенности объектов критической информационной инфраструктуры**

В результате изучения дисциплины студент должен:

**знать:**

- Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- Процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;



- Последствия инцидентов информационной и ядерной безопасности;

- Процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. **уметь:**

- выявлять и оценивать угрозы нсд к сетям электросвязи;
- анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы;
- проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации.

**Краткое содержание дисциплины (модуля)**

**Тема 1.** Цели, задачи и этапы создания и применения системы защиты.
**Тема 2.** Анализ уязвимости объектов и рисков потери ресурсов. Модели угроз. Модели нарушителей. Выявление и оценка основных видов угроз ИБ.
**Тема 3.** Управление ИБ в АСУ. Задачи УИБ. Модель технологического цикла управления средствами обеспечения безопасностью информации.
**Тема 4.** Формирование интегральной модели обеспечения ИБ в неоднородных АСУ.
**Тема 5.** Протоколы управления ключевой и парольной защитой. Основные положения концепции защиты объектов (ЗО) критической информационной инфраструктуры (КИИ).
**Тема 6.** Основные положения Федерального Закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктурой РФ». Категорирование объектов по степени угроз. Анализ рисков.
**Тема 7.** Модели оценки ценности развединформации. Общие принципы и состав систем обеспечения безопасности значимого объекта (организации, предприятия).
**Тема 8.** Методика определения критических процессов на объектах КИИ. Принципы защиты и построения защиты значимых объектов КИИ.
**Тема 9.** Модель угроз и технические каналы утечки информации. Безопасность информации, обрабатываемой на объектах КИИ. Общие принципы формирования модели угроз информационной безопасности (УИБ).
**Тема 10.** Выявление и анализ угроз информационной безопасности. Формирование и анализ модели нарушителя.
**Тема 11.** Цели и задачи технической разведки. Принцип организации и ведение технической разведки. Классификация технической разведки. Демаскирующие признаки.
**Тема 12.** Физические основы технических средств разведки. Основы противодействия техническим средствам разведки. Основные направления противодействия техническим средствам разведки. Основные положения системного подхода к защите значимых объектов КИИ.
**Тема 13.** Цели, задачи и ресурсы системы защиты информации. Угрозы ИБ и меры по их предотвращению. Определение угроз безопасности объектов КИИ.
**Тема 14.** Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Категорирование объектов КИИ. Системы безопасности значимых объектов (субъектов КИИ).
**Тема 15.** Стадии (этапы) работ по созданию систем безопасности. Проектирование системы безопасности значимых объектов. Комплексная политика защиты информации. Организация технической защиты информации и защиты значимых объектов КИИ.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Организационное и правовое обеспечение информационной безопасности»
10.05.03 «Информационная безопасность автоматизированных систем» специализация
«Безопасность открытых информационных систем»

**Объем дисциплины (модуля):** 4 зачетных единиц, 144 академических часов.

**Форма промежуточной аттестации:** Дифференцированный зачет (5 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

Задачи дисциплины– дать основы:

- информационного законодательства Российской Федерации;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- построения систем организационной защиты объектов информатизации

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

В результате изучения дисциплины студент должен:

Знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;
- понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
- правила лицензирования и сертификации в области защиты информации
- теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию;
- основные направления и методы организационной защиты информации в организациях с различными формами собственности
- основные положения международных стандартов в области информационной безопасности

Уметь:

- отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития;

Владеть:
- умением работы с нормативно-правовыми актами;
- умением разработки нормативно-методических материалов по регламентации системы организационной защиты информации;
- навыками применения различных способов методов защиты информации по каналам утечки и от несанкционированного доступа к ней;
- навыками проектирования систем защиты информации

В процессе освоения дисциплины формируются следующие компетенции:

- способность использовать нормативные правовые акты в своей профессиональной деятельности
- способность участвовать в разработке проектной и технической документации
- способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы
  • разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем

**Краткое содержание дисциплины (модуля)**
Тема 1. Законодательство РФ в сфере информационной безопасности
Тема 2. Практика правонарушений в области ИБ
Тема 3. Государственная система защиты информации РФ
Тема 4. Организация режима коммерческой тайны
Тема 5. Защита государственной тайны
Тема 6. Документация в области ИБ
Тема 7. Лицензируемая деятельность в области ИБ
Тема 8. Проектирование системы защиты информации
Тема 9. Аттестация объектов информатизации

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Основы построения защищенных компьютерных сетей для обучающихся по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем профиль: Безопасность открытых информационных систем форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** экзамен (6 семестр)

**Планируемые результаты освоения:** ОПК-10

Знать:
- Угрозы нарушения информационной безопасности компьютерных сетей.
- Основные криптографические методы защиты информации.
- Архитектуру и функции систем управления сетями, стандарты систем управления.
- Принципы функционирования защищенных сетевых протоколов.
- Средства мониторинга и анализа компьютерных сетей.
- Методы устранения неисправностей в технических системах.

Уметь:
- Применять основные протоколы и технологии обеспечения безопасности компьютерных сетей.
- Выполнять мониторинг и анализ работы локальной сети с помощью программноаппаратных средств.
- Осуществлять диагностику и поиск неисправностей всех компонентов сети.
- Выполнять действия по устранению неисправностей.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Программно-аппаратные средства защиты информации»
10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

**Объем дисциплины (модуля):** 8 зачетных единиц, 288 академических часов.

**Форма промежуточной аттестации:** Дифференцированный зачет (7, 8 семестры).

**Цели и задачи освоения дисциплины (модуля)**

Основной целью дисциплины «Программно-аппаратные средства защиты информации» является теоретическая и практическая подготовка работе с современными отечественными средствами защиты информации и внедрение их в систему защиты информации.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить типы и виды средств защиты информации;
- дать представление о существующих отечественных и зарубежных средствах защиты информации;
- научить устанавливать, настраивать и администрировать средства защиты информации;
- научить делать обоснованный выбор средства защиты информации при проектировании системы защиты информации.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем.

В результате изучения дисциплины студент должен:

знать:

- дополнительные источники получения информации по администрированию средств защиты;
- основные угрозы безопасности информации;
- требования к обеспечению ИБ различными техническими мерами;
- принципы работы и основной функционал средств защиты информации;
- порядок сертификации средств защиты информации в РФ;
- варианты и формы сертификации средств защиты информации в РФ;
- виды сертифицируемых средств защиты информации и предъявляемые им требования по безопасности;
- основные типы и виды средств защиты информации, принципы их действия;
- основные модули и функциональные возможности средств защиты информации;
- требования к среде функционирования средства защиты информации;
- принципы функционирования модулей средств защиты информации;

- способы влияния средств защиты информации на программное окружение;



- варианты зависимости работоспособности средств защиты информации от программного окружения;
- основные виды и типы средств защиты информации;
- основной функционал различных видов средств защиты информации;
- требования по обеспечению ИБ для различных ИС;
- правила выбора средств защиты информации в различных ИС;
- отечественные средства защиты информации; уметь:
- находить необходимую дополнительную информацию по средству защиты на сайте компании-производителя;
- сопоставлять реализуемый средствами защиты информации функционал с предъявляемыми требованиями по ИБ;
- определять нейтрализуемые средствами защиты информации угрозы;
- формулировать требования к конфигурированию средств защиты информации;
- выбрать необходимый способ сертификации средства защиты информации;
- составить план сертификации средства безопасности;
- определить состав требований, предъявляемых к сертифицируемому средству защиты информации и к компании-заявителю;
- настраивать среду функционирования перед установкой средств защиты информации;
  - устанавливать, настраивать и удалять средства защиты информации;
- применять различные конфигурации средств защиты информации в зависимости от параметров информационной системы;
- проводить проверку работоспособности средств защиты информации
- анализировать журнал событий средств защиты информации;
- осуществлять сохранение настроек средства защиты информации и их восстановление;
- поиск причин нарушения работоспособности средства защиты информации;
- определить виды средств защиты информации в зависимости от предъявляемых требований;
- обоснованно подобрать необходимые модели и марки средств защиты информации;

**Краткое содержание дисциплины (модуля)**

Тема 1. Классификация и виды средств защиты информации.
Тема 2. Система сертификации средства защиты информации в РФ.
Тема 3. Средства доверенной загрузки.
Тема 4. Средства защиты от несанкционированного доступа.
Тема 5. Средства криптографической защиты информации.
Тема 6. Средства антивирусной защиты.
Тема 7. Средства анализа и контроля защищенности.
Тема 8. Выбор технических мер при проектировании системы защиты информации.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
**«РАЗРАБОТКА И ЗАЩИТА WEB-ПРИЛОЖЕНИЙ»**
Специальность: 10.05.03 «Информационная безопасность автоматизированных систем» специализация: «Безопасность открытых информационных систем» форма обучения очная

**Объем дисциплины (модуля):** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет.

**Цели и задачи освоения дисциплины (модуля)**

Целью дисциплины «Разработка и защита web-приложений» является обучение студентов основам создания веб приложений, ознакомиться с современным серверным и сетевым оборудованием, изучить методики и способы защиты веб приложений и сетевого оборудования.

Задачи дисциплины «Разработка и защита web-приложений»:

- изучить устройство сети Интернет;
- изучить языки разметки документов;
- изучить протоколы http, https, ftp;
- изучить принцип работы веб сервера;
- принципы функционирования веб приложений;
- изучить средства разработки веб приложений;
- изучить наиболее распространённые веб серверы, их возможности и функционал;
- научиться создавать простейшие веб страниц;
- научиться использовать основные и дополнительные метатеги;
- изучить способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- изучить методы проверки и тестирования законченных сайтов;
- изучить подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием;
- научиться организовывать способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование;
- рассмотреть наиболее распространенные типы уязвимостей на сетевое оборудование;
- научиться настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта;
- научиться настраивать межсетевые экраны, коммутаторы, балансировку нагрузки;
- научиться организовывать серверные кластеры;
- научиться производить анализ защищенности веб приложения;  научиться организовывать защиту веб приложений.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7 – способностью создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

В результате изучения дисциплины студент должен:

**Знать:**

- устройство сети Интернет;
- языки разметки документов;
- протоколы http, https, ftp;
- принцип работы веб сервера;
- принципы функционирования веб приложений;
- средства разработки веб приложений;
- наиболее распространённые веб серверы, их возможности и функционал;
- способы создания простейших веб страниц;
- основные и дополнительные метатеги;
- способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- методы проверки и тестирования законченных сайтов;
- подходы к проектированию веб сервера и локально-вычислительной сети с сетевым оборудованием;
- способы защиты от различного рода сетевых атак на Web и DNS серверы, и сетевое оборудование;
- наиболее распространенные типы уязвимостей.

**Уметь:**

- использовать средства разработки веб приложений;
- разрабатывать простые веб страницы на языке html;
- использовать основные и дополнительные метатеги;
- использовать дополнительный инструментарий, позволяющий увеличивать число посетителей и продвигать сайт в поисковых системах;
- настраивать веб сервер и его сетевые карты, роли DNS, IIS и другие для корректной работы сайта;
- настраивать межсетевые экраны, коммутаторы, балансировку нагрузки; организовывать серверные кластеры;
- производить анализ защищенности веб приложения;
- производить защиту веб приложения; производить устранение основных типов угроз.

**Краткое содержание дисциплины (модуля) 5 семестр**

**Тема 1.** Введение. Устройство сети Интернет. Обзор современных веб технологий.

**Тема 2.** DNS сервер и его роль в организации работы сайта.

**Тема 3.** DNS записи, маршрутизация и обзор современных DNS серверов.

и пересылки запросов DNS. Для этого: 1. Используя любую редакцию ОС MS Windows Server, выполнить настройки сетевого адаптера и присвоить ему статический IP-адрес. 2. Установить роль DNS. 3. Создать одну зону прямого просмотра (имя зоны назначаете самостоятельно). 4. Внести соответствующие записи необходимых типов в базу DNS. 5. Настроить зону обратного просмотра. 6. Организовать передачу зоны на другой доверенный сервер.

**Тема 4.** Языки разметки документов. Гипертекстовая разметка XML.

**Тема 5.** Средства разработки веб приложений. CMS – Системы управления контентом веб-сайтов.

**Тема 6.** Протокол HTTP, веб сервер и веб клиент, прокси сервер.

**Тема 7.** Создание простой web-страницы. Форматирование.

**Тема 8.** Каскадные таблицы стилей (CSS).
**Тема 9.** Метатеги основные и дополнительные.
**Тема 10.** Системы индексации сайтов. Файл robots.txt и sitemap.xml.
**Тема 11.** Веб-аналитика. Счетчики.



**Тема 12.** JavaScript для WEB.

**6 семестр**
**Тема 13.** Защищенное делегирование с DNSSEC.
**Тема 14.** Межсетевые экраны. Настройка межсетевого экрана модели DFL-860e.
**Тема 15.** Способы реализации процесса балансировки нагрузки.
**Тема 16.** Веб сервер и DNS сервер. Виртуализация серверов и ролей.
**Тема 17.** Почтовый сервер. Принцип работы, настройка и администрирование.
**Тема 18.** Способы защиты от спама.
**Тема 19.** Организация антивирусной защиты на серверах и шлюзах.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

## РАЗРАБОТКА И ЗАЩИТА ОТКРЫТЫХ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рабочая программа для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (9 семестр)

**Планируемые результаты освоения:**

ОПК-5.3

Перечень планируемых результатов обучения по дисциплине (модулю):

Знать:

- основные законы, нормативно-правовые акты в области защиты врачебной тайны и персональных данных;
- принципы проектирования защищённых медицинских систем;
- методы внедрения, сопровождения и совершенствования защищённых медицинских систем;
- методы анализа эффективности работы системы защиты информации медицинских информационных систем.

Уметь:

- определять уровень защищённости информационной системы персональных данных и класс государственной информационной системы;
- обеспечивать защиту врачебной тайны и персональных данных в соответствии с законами, нормативно-правовыми актами Российской Федерации;
- выбирать и обосновывать инструментарий разработки защищённых медицинских систем;
- проектировать защищённые медицинские информационные системы;
- внедрять, сопровождать и совершенствовать защищённые медицинские системы;
- проводить анализ эффективности работы системы защиты информации медицинских информационных систем.

Владеть:

- навыками определения уровня защищённости информационной системы персональных данных и класса государственной информационной системы;
- навыками обеспечения защиты врачебной тайны и персональных данных в соответствии с законами, нормативно-правовыми актами Российской Федерации;
- навыками выбора и обоснования инструментария разработки защищённых медицинских систем;
- навыками проектирования защищённых медицинских информационных систем;

- навыками внедрения, сопровождения и совершенствования защищённых медицинских систем;
- навыками анализа эффективности работы системы защиты информации медицинских информационных систем.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины (модуля):** 8 зачетных единиц.

**Форма промежуточной аттестации:** дифференцированный зачет, экзамен.

**Цели и задачи освоения дисциплины (модуля)**

Целью дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» является обучение студентов основам проектирования защищенных автоматизированных систем, ознакомление с оборудованием и организации защиты датчиков, автоматизированных узлов и диспетчерских.

Задачи дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»:

- изучить современные технологические процессы и их технологию;
- основную нормативно-техническую документацию;
- изучить виды оборудования и принципы работы;
- изучить всевозможные угрозы, влияющие на работу оборудования и технологического процесса в целом;
- научиться строить модели нарушителя для предложенной технологической линейки или технологии;
- научиться настраивать оборудование;
- научиться строить принципиальные и подробные электрические схемы, в том числе с использованием эмуляторов и имитационных тренажеров;
- научиться разрабатывать мнемосхемы и скада системы для предложенного технологического процесса.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2 – Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

**<u>Разработка и эксплуатация автоматизированных систем в защищенном исполнении 1</u>**

В результате изучения дисциплины студент должен: **знать:**

- нормативно-техническую документацию;
- принцип работы оборудования автоматизированных систем;
- программное обеспечение для моделирования технологических процессов;
- способы проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса; • методики чтения технологических схем;
- программное обеспечение для проектирования схем автоматизированных систем и узлов

**уметь:**

- работать с нормативно-технической документацией;



- применять навыки для проведения анализа, а также подбора оборудования и средств защиты для предложенного технологического процесса;
- анализировать предложенные структурные и принципиальные технологические схемы и сети автоматизированных систем и узлов;
- работать с программным обеспечением для проектирования схем автоматизированных систем и узлов;
- проводить экспериментально-исследовательские работы с оборудованием и сетями автоматизированных систем.

**Разработка и эксплуатация автоматизированных систем в защищенном исполнении 2**

В результате освоения ОП выпускник должен: **знать:**

- основные понятия систем видеонадения;
- нормативно-техническую документацию;
- основные понятия аппаратных средств систем видеонаблюдения;
- основные подходы к проектированию при совместном использовании видеоаналитики и систем видеонаблюдения;
- процессы обработки сигналов изображений в интеллектуальной видеосистеме;
- методы визуализации в интеллектуальных видеосистемах.

**уметь:**

- разрабатывать проекты систмем видеонаблюдения с видеоаналитикой;
- обучать системы видеонаблюдения и адптировать их под конкретные задачи;
- выполнять подбор оборудования и программного обеспечения под конкретные задачи.

**Краткое содержание дисциплины (модуля)**

**Тема 1.** Введение. Обзор современных автоматизированных систем и устройств.
**Тема 2.** Система теплоснабжения зданий различного назначения. Учет и регулировка теплоносителя.
**Тема 3.** Тепловые счетчики, их устройство и режимы работы.
**Тема 4.** Интерфейсы RS-232, RS-422 и RS-485.
**Тема 5.** Система погодного регулирования. Система управления газовыми и твердотопливными котлами.
**Тема 6.** ТРМ32 контроллер для отопления и ГВС. СУНА-121 контроллер для групп насосов. Угрозы и аварийные ситуации.
**Тема 7.** Установки и устройства для поддержания микроклимата в помещениях/зданиях различного назначения. Модели угроз.
**Тема 8.** Системы охранно-пожарной сигнализации и пожаротушения. Организация диспетчерских пультов.
**Тема 9.** Системы видеонаблюдения. Проектирование сетей охранного телевидения. Виды оборудования. Защита данных.
**Тема 10.** Системы диспетчеризации. Их обустройство. Принципиальные схемы.
**Тема 11.** Среда проектирования Codesys. Алгоритмы работы контроллера ПЛК-150.
**Тема 12.** Принципы конфигурирования оборудования автоматизации.
**Тема 13.** Моделирование сетей и узлов систем автоматизации в различных средах. Имитационные модели.
**Тема 14.** Разработка Скада-систем.

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Сети и системы передачи информации для обучающихся по направлению подготовки (специальности)
10.05.03 Информационная безопасность автоматизированных систем
Профиль: Безопасность открытых информационных систем
Форма обучения: очная
Специалитет

**Объем дисциплины:** 8 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (4 семестр), экзамен (5 семестр).

**Планируемые результаты освоения:** ОПК-9,
УК-2

В результате изучения дисциплины студент должен:

Знать:

– Принципы связи и обмен данными в локальной проводной сети;
– Уровни доступа и распределения в сети Ethernet;
– Структуру сети Интернет, принципы обмена данными между узлами в Интернет;
– Схему подключения к Интернету через поставщика услуг;
– Сетевые устройства;
– Виды, характеристики и маркировку сетевых кабелей и контактов;
– Принципы сетевой адресации, формат IP-адреса и маски подсети, типы IP-адресов и методы их получения, протокол DHCP;
– Многоуровневую модель межсетевого взаимодействия OSI и сетевые протоколы;
– Беспроводные технологии для локальных сетей;
–Основные сетевые службы, архитектуру клиент-сервер, IP-сервисы и принципы их работы, сервис электронной почты, сервис доменных имен DNS; – Архитектуру и возможности систем Cisco IOS / Huawei VRP;
– Основные протоколы маршрутизации;
– Структуру IP-адресации в ЛВС;
–Методы трансляции адресов NAT и PAT;
– Базовые настройки маршрутизаторов;
– Базовые настройки коммутаторов;
– Механизмы резервного копирования и аварийного восстановления в сети.

Уметь:

– Проектировать и устанавливать домашнюю сеть или сеть малого предприятия, а также подключать ее к сети Интернет;
– Выполнять проверку и устранять неполадки сети и подключения к сети Интернет; – Обеспечивать общий доступ нескольких компьютеров к сетевым ресурсам (файлам, принтерам и др.);
– Выявлять и устранять угрозы безопасности локальной компьютерной сети;
– Настраивать и проверять базовые Интернет-приложения;

– Настраивать базовые IP-сервисы при помощи графического интерфейса ОС;
– Устанавливать и настраивать устройства для подключения к сети Интернет и серверам, выполнять поиск и устранение неполадок;
–Проектировать базовую проводную инфраструктуру для поддержки сетевого трафика;
– Обеспечивать подключение к сети WAN на базе сервисов телекоммуникационных компаний;
– Выполнять адекватные процедуры восстановления при авариях и осуществлять резервирование сервера;
– Контролировать производительность сети и выявлять сбои;
–Выявлять и устранять неполадки с использованием структурированной многоуровневой процедуры.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«**Системы видеонаблюдения**»
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины (модуля):** 8 зачетных единиц.

**Форма промежуточной аттестации:** дифференцированный зачет, экзамен.

**Цели и задачи освоения дисциплины (модуля)**

Целью дисциплины «Системы видеонаблюдения» является обучение студентов основам проектирования систем видеонаблюдения, ознакомиться с современным оборудованием, изучить методики расчета и подбора оборудования, изучить технологические схемы, используемые в сблокировке с охранно-пожарными и другими системами. Задачи дисциплины «Системы видеонаблюдения»:

- изучить основную нормативно-техническую документацию;
- изучить основные принципы и подходы при организации технической защиты информации;
- изучить методики расчета и подбора оборудования видеонаблюдения;
- изучить архитектуру сетей видеонаблюдения;
- изучить некоторое сервисное программное обеспечение.
- изучить принципы и подходы к проектированию систем видеонаблюдения.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-9 – способностью решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

**Системы видеонаблюдения 1**

В результате изучения дисциплины студент должен: **знать:**

- основные понятия систем видеонаблюдения;
- нормативно-техническую документацию;
- основные понятия аппаратных средств систем видеонаблюдения;
- основы базовых технологий систем видеонаблюдения; • принцип работы устройств видеонаблюдения; **уметь:**
- формализовать поставленную задачу;
- осуществлять аппаратную реализации состава системы;
- проектировать сети систем видеонаблюдения;
- осуществлять настройку систем видеонаблюдения;
- проводить анализ и монитоинг сетей и узлов видеонаблюдения.

**Системы видеонаблюдения 2**

В результате освоения ОП выпускник должен: **знать:**

- основные понятия систем видеонадения;
- нормативно-техническую документацию;



- основные понятия аппаратных средств систем видеонаблюдения;

- основные подходы к проектированию при совместном использовании видеоаналитики и систем видеонаблюдения;
- процессы обработки сигналов изображений в интеллектуальной видеосистеме;
- методы визуализации в интеллектуальных видеосистемах.

**уметь:**

- разрабатывать проекты систмем видеонаблюдения с видеоаналитикой;
- обучать системы видеонаблюдения и адптировать их под конкретные задачи;
- выполнять подбор оборудования и программного обеспечения под конкретные задачи.

**Краткое содержание дисциплины (модуля)**

**Тема 1.** Введение. Назначение систем видеонаблюдения и их роль. Действующая нормативная документация. Федеральные законы.
**Тема 2.** Знакомство со средой автоматизированного проектирования AutoCad.
**Тема 3.** Знакомство и изучение реальных проектов и их технических решений.
**Тема 4.** Классификация систем видеонаблюдения. Общие требования, предъявляемые к системам видеонаблюдения.
**Тема 5.** Виды видеокамер и их устройство. Интерфейсы. Способы настройки и управления. Правила подбора. Датчики, сблокированные с камерами.
**Тема 6.** Виды объективов для видеокамер. Методика расчета и подбор.
**Тема 7.** Инфракрасные прожекторы, их расчет и подбор.
**Тема 8.** Кожухи и корпуса видеокамер камер. Обеспечение микроклимата. Методика расчета и подбор.
**Тема 9.** Виды видеорегистраторов. Правила подбора. Настройка.
**Тема 10.** Делитель экрана. Мультиплексор. Платы видеозахвата.
**Тема 11.** Сетевое оборудование для систем видеонаблюдения. Правила подбора. Расчет пропускной способности каналов.
**Тема 12.** Источники резервированного питания. Методика подбора. Расчет общей нагрузки. Привязка оборудования к индивидуальному или к центральному источнику питания.
**Тема 13.** Оборудование АРМ. Пульты управления. Программные средства регистрации видеосигнала.
**Тема 14.** Типовые схемы видеонаблюдения. Простейшие схемы с одним видеорегистратором. Сложные схемы. Схемы, комбинированные с охранно-пожарной сигнализацией, системой СКУД и климатическим оборудованием.

Аннотация к рабочей программе дисциплины

**Системы управления базами данных**

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем

Уровень высшего образования: специалитет форма обучения

очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** экзамен (5 семестр).

**Планируемые результаты освоения:** ОПК-14

В результате освоения дисциплины студент должен:

знать

- типологию и методологию проектирования баз данных, уметь классифицировать информационные задачи, решаемые с использованием баз данных;
- особенности моделирования и проектирования реляционных баз данных;
- о целях и средствах разработки и администрирования баз данных; уметь

- применять навыки разработки баз данных на практике;

иметь навыки

- владения системным подходом как методологической основой проектирования информационных систем, использующих базы данных; • владения методикой составления запросов на языке SQL.

**Цели и задачи освоения дисциплины:**

Цель: формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с проектированием и реализацией прикладных защищенных решений и баз данных под управлением современных систем управления базами данных (СУБД).

Задачи:

-дать общее представление о системе управления базами данных как об одной из основных составляющих эффективных систем автоматизированной обработки информации;

-изучить паттерны проектирования баз данных для различных прикладных задач;

-изучить характеристики и типы систем баз данных, области применения систем управления базами данных в разрезе CAP-теоремы;

-рассмотреть вопросы транзакционной целостности данных, способы масштабирования для высоконагруженных и распределённых систем;

-рассмотреть область применимости СУБД с различными моделями данных: объектнореляционной, объектной, графовой, колоночной, документоориентированной, ключ-значение;

-изучить внутреннюю организацию СУБД в части хранения на диске и в памяти, особенности организации индексов, а также инженерные подходы к оценке и выбору СУБД.

**Краткое содержание дисциплины:**

Дисциплина включает 8 разделов:

1. Введение.
2. Организация современной СУБД.
3. Логические модели данных.
4. Нормализация данных в реляционной модели.
5. Язык запросов SQL: оконные функции, специальные конструкции.
6. Древововидные структуры. Реализация в реляционной модели. Рекурсивые запросы SQL.
7. Оптимизация выполнения запросов.
8. Сравнение производительности СУБД.

Аннотация к рабочей программе дисциплины

**Теоретико-числовые методы в криптографии**

Специальность:10.05.03 Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем форма обучения очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачёт (7 семестр).

**Планируемые результаты освоения: ОПК-3**

знать:

- об основных задачах и понятиях криптографии;
- о теоретико-числовых основах двухключевой криптографии;
- основы дискретной алгебры и теории чисел;
- основные виды асимметричных криптографических алгоритмов;
- алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.

уметь:

- проводить оценку сложности алгоритмов;
- корректно применять асимметричные криптографические алгоритмы;
- формализовать поставленную задачу;
- выполнить постановку задач криптоанализа и указать подходы к их решению; • использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов.

владеть:

- криптографической терминологией;
- навыками применения алгоритмов, основанных на теоретико-числовых принципах, к вопросам построения криптосистем и их анализу;
- навыками использования современной научно-технической литературы в области криптографической защиты
- навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов

**Цели и задачи освоения дисциплины:** Изучаются основы теории чисел: теория делимости, теория сравнений, теория квадратичных сравнений, конечные группы, кольца и поля вычетов, порядок элемента в мультипликативной группе, порождающий элемент мультипликативной группы вычетов.

Изучаются приложения теории чисел в криптографии: тесты на простоту числа, доказуемо простые числа, асимметричные криптосистемы: RSA, Эль-Гамаля, Рабина, DSA, ГОСТ Р 34.11-94, Гольдвассер-Микали, Блюма-Гольдвассер, Шамира и др., вопросы условной криптографической стойкости этих систем, проблемы факторизации и дискретного логарифмирования, алгоритмы для решения этих проблем.

**Краткое содержание дисциплины:**

Основные понятия теории чисел. Теорема делимости. Наибольший общий делитель и алгоритм Евклида. Цепные дроби. Наименьшее общее кратное. Простые числа. Теоремы Евклида о простых числах. Решето Эратосфена. Основные свойства простых чисел. Теорема о единственности разложения на простые сомножители. Теорема о делителях числа и ее следствия. Асимптотический закон распределения простых чисел. Функция Эйлера, ее свойства. Сравнения. Свойства сравнений. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент. Теорема Эйлера, теорема Ферма. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайкла. Применение теоремы Ферма в криптосистеме RSA. Сравнения с одним неизвестным 1-й степени. Система сравнений 1-й степени. Китайская теорема об остатках. Применение Китайской теоремы об остатках в RSA Квадратичные сравнения по простому модулю. Символ Лежандра и его свойства. Решение квадратичных сравнений по простому модулю. Число решений квадратичного сравнения по составному модулю. Символ Якоби, его свойства. Тест Соловея-Штрассена. Квадратичные сравнения по модулю RSA. Связь задач извлечения корней и факторизации. Криптосистема Рабина. Квадраты и псевдоквадраты. Числа Блюма. BBS-генератор. Криптосистема БлюмаГольдвассер, криптосистема Гольдвассер-Микали. Тест Миллера-Рабина. Порядок группы. Порядок элемента в группе. Порождающий элемент. Существование порождающего элемента в $Z^*_n$. Критерий Люка. Теорема Сэлфриджа и тест Миллера. Теорема Поклингтона и тест на простоту на ее основе. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна. Тест Лукаса-Лемера. Теорема Диемитко. Процедура генерации простых чисел ГОСТ Р 34.10-94. Дискретный логарифм. Проблема Диффи-Хелмана. Криптосистема Эль-Гамаля. Проблема факторизации. Метод пробных делений. Метод Ферма факторизации.
Метод квадратичного решета. Ро-метод Полларда факторизации. p—1 – метод факторизации. Метод Диксона. Задача дискретного логарифмирования. Метод прямого поиска. Ро-метод Полларда дискретного логарифмирования. Алгоритм Полига-Хеллмана. Метод «Шаг младенца-шаг великана». Метод исчисления порядка.

Аннотация к рабочей программе дисциплины
Технологии и методы программирования
Специальность: 10.05.03. Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем форма обучения
очная

**Объем дисциплины (модуля):** 8 з.е.
**Форма промежуточной аттестации:** дифференцированный зачет(5,6 семестры).
**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Технологии и методы программирования» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

**Основной целью** дисциплины «Технологии и методы программирования» является изложение основополагающих принципов разработки программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

**Задачи** дисциплины «Технологии и методы программирования»

• дать представление о компьютерных технологиях и методах программирования;
• научить использовать компьютерные технологии и методы программирования для решения разнообразных прикладных задач.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-7 - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

.

В результате изучения дисциплины студент должен: знать:

- основные языки и системы программирования, среды разработки и компьютерные технологии;
- способы построения, анализа и реализации алгоритмов.

уметь:

- применять основные языки и системы программирования, среды разработки и компьютерные технологии в профессиональной деятельности;
- проводить построение, анализ и реализацию алгоритмов в современных программных комплексах.

**Краткое содержание дисциплины (модуля)**
**5 семестр**

1. Введение в дисциплину
2. Разработка с использованием скриптовых языков программирования.
3. Разработка Win32 приложений и библиотек
4. Разработка консольных приложений
5. Разработка оконных приложений
6. Параллельное программирование

7. Разработка и использование COM объектов
8. Разработка и использование ActiveX объектов

**6 семестр**

1. Разработка сетевых приложений
2. Разработка сервисных приложений
3. Разработка .NET-приложений
4. Разработка внешних хранимых процедур для серверов баз данных
5. VBA приложения
6. Web приложения

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью
специальность 10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем» форма обучения
очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (10 семестр)

**Планируемые результаты освоения:**

ОПК-1, 11

Знать:

- основные задачи и понятия ИБ;
- основные стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием

Уметь:

- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

Владеть:

- терминологией и процессным подходом построения систем управления ИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Электроника и схемотехника для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (6 семестр)

**Планируемые результаты освоения:**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

Знать:

- терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем;
- основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах; основные параметры и принципы работы базовых функциональных элементов радиоэлектроники (усилителей, генераторов и т.п.);
- основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств;
- основные подходы к решению практических задач, связанных с анализом сигналов в частотной области.

Уметь:

- проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем;
- оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований;
- рассчитывать простые аналоговые и цифровые радиоэлектронные устройства;
- применять современную вычислительную технику при анализе и разработке аналоговых и цифровых электронных устройств.

Владеть:

- приемами и навыками решения конкретных задач из разных областей электроники и схемотехники;

- основными математическими методами анализа и расчета электрических цепей и сигналов;

базовыми навыками проектирования, конструирования, монтажа и наладки простых радиоэлектронных устройств.

Аннотация к рабочей программе дисциплины

**Основы построения защищенных баз данных**

Специальность: 10.05.03. Информационная безопасность автоматизированных систем

Специализация: Безопасность открытых информационных систем

Уровень высшего образования: специалитет форма обучения

очная

**Объём дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** экзамен (7 семестр).

**Планируемые результаты освоения:** ПК-6

В результате освоения дисциплины студент должен:

**знать:**

- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД;
- нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; - принципы построения систем защиты информации;

**уметь:**

- анализировать и оценивать угрозы информационной безопасности объекта; - применять действующую законодательную базу в области обеспечения безопасности систем баз данных;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;
- формализовать поставленную задачу по обеспечению защиты БД;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- использовать средства защиты, предоставляемые системами управления базами данных;
- проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований; **владеть:**
- методиками использования средств защиты, предоставляемых системами управления базами данных;
- профессиональной терминологией в области информационной безопасности;
- практическими навыками работы с научно-технической документацией;
- навыками разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем;
- навыками разработки частных политик безопасности, в том числе политик управления доступом и информационными потоками;
- методами анализа безопасности информационных систем на базе промышленных СУБД;
- навыками формирования требований по защите информации.

**Цели и задачи освоения дисциплины:**

Цель: формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных, а также связанных с обеспечением безопасности информации в автоматизированных информационных системах, основу которых составляют базы данных, а также с навыками работы со встроенными в системы управления базами данных средствами защиты.

Задачи:

-обучить студентов принципам работы современных систем управления базами данных;
-привить студентам навыки проектирования и реализации баз данных;
-приобретение системного подхода к проблеме защиты информации в СУБД;
-изучение моделей и механизмов защиты в СУБД;
-приобретение практических навыков организации защиты БД;
-обучить студентов проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
-обучить студентов формализовать поставленную задачу по обеспечению защиты БД;
-обучить студентов применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
-привить студентам навыки разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в СУБД.

**Краткое содержание дисциплины:**

Дисциплина включает 8 разделов:

1. Введение. Информационные системы СУБД.
2. Целостность БД и способы ее обеспечения. Первичные ключи. Индексирование в базах данных. Оптимизация запросов.
3. Первичные ключи. Индексирование в базах данных. Оптимизация запросов.
4. Транзакции и блокировки. Средства идентификации и аутентификации.
5. Средства управления доступом. Шифрование в СУБД.
6. Критерии защищенности БД. Безопасность БД, угрозы, защита.
7. Модели безопасности в СУБД. Классификация угроз конфиденциальности СУБД.
8. Аудит и подотчетность. Обзор. Другие программно-технические способы защиты информации.

ФГАОУ ВО «ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Проектирование и внедрение систем защиты информации»
10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

**Объем дисциплины (модуля):** 4 зачетных единиц, 144 академических часов.

**Форма промежуточной аттестации:** Дифференцированный зачет (6 семестр).

**Цели и задачи освоения дисциплины (модуля)**

Цель дисциплины « Проектирование и внедрение систем защиты информации»: закрепление теоретических знаний и практических навыков в области построения, разработки и внедрения систем защиты информации для различных информационных систем.

Основными задачами дисциплины являются:

- изучение требований ГОСТов и НПА по проектированию СЗИ;
- изучение возможностей и освоение функционала различных инструментов по проектированию СЗИ;
- формирование требований к проектируемой системе защиты информации с учетом анализа угроз;
- разработка технического задания и технического проекта на создание системы защиты информации.

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-4. Способен выполнять комплекс мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД.

В результате изучения дисциплины студент должен:

**Знать**

- общие принципы построения и внедрения систем защиты информации для автоматизированных систем;
- необходимые для проектирования ГОСТы и НПА;
- принципы проектирования архитектуры, структуры и основных объектов защищаемых автоматизированных систем;
- основные этапы процесса проектирования и методы, используемые при построении проектируемой системы защиты информации.

**Уметь**

- формировать требования к проектируемой системе защиты информации с учетом анализа угроз;
- составлять функциональные схемы проектируемой СЗИ и АС.

**Владеть**

- методами построения защищенных автоматизированных систем;
- навыками составления, технического задания, технического проекта и пониманием содержания основных этапов процесса проектирования.

**Краткое содержание дисциплины (модуля)** Дисциплина
включет 6 тем:
Тема 1. Основные термины и понятия дисциплины.
Тема 2. Этапы проектирования СЗИ
Тема 3. Определение требований к СЗИ
Тема 4. ГОСТы по разработки и проектированию СЗИ
Тема 5. Инструментарий по проектированию СЗИ
Тема 6. Разработка технического задания и технического проекта на создание СЗИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Разработка и защита мобильных приложений»
10.05.03 Информационная безопасность автоматизированных систем
Профиль: Безопасность открытых информационных систем
(связь, информационные и коммуникационные технологии)
Форма обучения очная

**Объем дисциплины (модуля):** 4 зачетных единиц.

**Форма промежуточной аттестации:** дифференцированный зачет.

**Цели и задачи освоения дисциплины (модуля)**

Разработка и защита мобильных приложений обеспечивает приобретение знаний и умений в соответствии с Федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Разработка и защита мобильных приложений» - является изложение теоретических и практических принципов разработки и защиты мобильных приложений с учетом современных тенденций.

Задачи курса - изучение:

- устройства платформы Android
- системного подхода к проектированию и созданию мобильных приложений
- архитектуры мобильного приложения, основных его компонентов
- основ разработки интерфейсов мобильных приложений
- основ разработки многооконных приложений
- основ работы с базами данных SQLite
- предотвращения угроз безопасности мобильных приложений

**Планируемые результаты освоения**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-5: Способен разрабатывать и проводить отладку программного кода

В результате освоения дисциплины студент должен

Знать:

- этапы и тенденции развития программирования, способы применения ИТ при разработке мобильных приложений.
- особенности применения сервисных программ и оболочек при разработке мобильных приложений.
- содержание рынка программных продуктов и информационных услуг, тенденции, развитие и особенности рынка.

Уметь:

• выбрать оптимальный программный продукт и модели информационных технологий из нескольких возможных для решения прикладной задачи, и провести сравнительную оценку эффективности.



• выбрать программный продукт и технологии для решения задачи с учетом конкретной предметной области и провести анализ эффективности использования ПО для решения задач в предметной области.

• разрабатывать сервисные программы и сервисные оболочки при разработке мобильных приложений с учетом конкретной предметной области.

Иметь навыки:

• применения информационных технологий и творческого подхода при решении стандартных и нестандартных задач

• выбора программных продуктов и мобильных технологий для решения задачи.

• использования сервисных программ и сервисных оболочек при разработке мобильных приложений для решения задачи.

**Краткое содержание дисциплины (модуля)**

1. Обзор платформ (ОС) для мобильных устройств и средств разработки под различные платформы. Android - история, инструментарий разработчика, архитектура ОС, структура и компоненты приложения. iOS - история, инструментарий разработчика, архитектура ОС, структура и компоненты приложения. Windows Phone - история, инструментарий разработчика, архитектура ОС, структура и компоненты приложения. BlackBerry - история, инструментарий разработчика, архитектура ОС, структура и компоненты приложения. Введение в разработку мобильных приложений
2. Архитектура приложений для Android. Ресурсы приложения. Пользовательский интерфейс. Инструментарий разработки приложений для Android: Android Studio, Android NDK. Эмуляторы Android. Основные виды Android-приложений. Обеспечение безопасности. Архитектура приложения, основные компоненты: Activities, Services, Content Providers, Broadcast Receivers. Манифест приложения. Ресурсы
3. Основы разработки интерфейсов мобильных приложений
4. Основы разработки многооконных приложений
5. Использование возможностей смартфона в приложениях
6. Использование библиотек
7. Работа с базами данных
8. Работа с графикой и анимацией.

Аннотация к рабочей программе дисциплины
Защита программ и данных
Специальность: 10.05.03. Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем форма обучения
очная

**Объем дисциплины (модуля):** 4 з.е.
**Форма промежуточной аттестации:** экзамен (9 семестр).
**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Защита программ и данных» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Защита программ и данных» является изложение основополагающих принципов защиты программ и данных. Задачи дисциплины «Защита программ и данных»:

- дать представление об основных угрозах для программ и данных;
- научить оценивать уровень защищенности программ и данных;
- дать основы системного подхода к обеспечению безопасности программ и данных

**Планируемые результаты освоения**
**В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:**

ПК-1. Способен разрабатывать и проводить отладку программного кода

В результате изучения дисциплины студент должен:
В результате освоения дисциплины студент должен

Знать

- понятия процессор, машинные команды, оперативная память, регистры, смещение, сегмент, разрядность, прерывание,
- основные машинные команды сложения (8086)
- основные машинные команды вычитания (8086)
- основные машинные команды умножения(8086)
- основные машинные команды деления (8086)
- основные машинные команды битовой арифметики (8086)
- низкоуровневой адресации (8086)
- знать способы создания побочных эффектов программы, позволяющие скрыть затруднить отладку
- современные средства защиты ПО
- основные виды закладок ПО • основные способы анализа ПО.

Уметь

- разрабатывать простые программы на языке ассемблер
- понимать логику работы программы на языке ассемблер
- определять основные побочные эффекты программы, позволяющие скрыть затруднить отладку
- использовать современные средства защиты ПО.

Владеть

- методами создания побочных эффектов программы, позволяющие скрыть затруднить отладку
- современными методами защиты ПО

- методами отладки и анализа ПО.

**Краткое содержание дисциплины (модуля)**

Введение в анализ ПО
Статический и динамический методы анализа ПО
Статический и динамический методы анализа ПО
Особенности анализа некоторых видов ПО
Инструменты анализа ПО
Защита программ от анализа
Модели взаимодействия программных закладок с атакуемой системой Методы внедрения программных закладок.

Аннотация к рабочей программе дисциплины
Интернет вещей
Специальность: 10.05.03. Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем форма обучения
очная

**Объем дисциплины (модуля):** 4 з.е.
**Форма промежуточной аттестации:** экзамен (8 семестр).
**Цели и задачи освоения дисциплины (модуля)**

Учебная дисциплина «Интернет вещей» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Интернет вещей» является изложение основополагающих принципов защиты программ и данных. Задачи дисциплины «Интернет вещей»:

- дать представление об основных угрозах для программ и данных;
- научить оценивать уровень защищенности программ и данных;
- дать основы системного подхода к обеспечению безопасности программ и данных

**Планируемые результаты освоения**
**В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:**
ПК-7. Способен организовывать и проводить работы по технической защите информации;

Знать
- основные типы оборудования используемого в проектах интернета вещей
- основные типы микроконтроллеров и микрокомпьютеров интернета вещей, их особенности, достоинства и недостатки
- основы разработки программного обеспечения в среде Arduino Studio
- наиболее распространенные типы сетей интернета вещей

Уметь
- формализовать поставленную задачу
- разбивать проект на функционально независимые блоки
- корректно подбирать необходимое оборудование
- разрабатывать алгоритм работы

Владеть
- терминологией Интернета Вещей
- навыками разработки решений Интернета Вещей
- навыками разработки программ (скетчей) Интернета Вещей

**Краткое содержание дисциплины (модуля)**

Микрокомпьютеры
Датчики и исполнительные устройства
Разработка проектов на базе Arduino
Механизмы сетевого взаимодействия устройств интернет вещей

# АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ
Рабочая программа для
обучающихся по специальности
10.05.03. Информационная безопасность автоматизированных систем
специализация «Безопасность открытых информационных систем»
форма обучения очная

**Объем дисциплины:** 4 з.е.

**Форма промежуточной аттестации:** дифференцированный зачет (10 семестр)

**Планируемые результаты освоения:**

ПК-2,3

Перечень планируемых результатов обучения по дисциплине (модулю):

**Знать:**
- Теоретические основы кредитно-финансовых операций и принципов работы антифрод систем;
- Законодательные и нормативно-правовые требования к защите кредитно-финансовых систем;
- Архитектуру антифрод систем;
- Основные векторы атак и способы защиты от них в рамках кредитно-финансовых систем.

**Уметь:**
- Проектировать систему защиты кредитно-финансовых систем;
- Формировать пакет документов для защиты кредитно-финансовых систем на основе требований законодательства РФ и нормативно-правовой базы.

**Владеть:**
- Навыками настройки и эксплуатации антифрод систем;
- Навыками управления информационной безопасностью в кредитно-финансовых системах на основе анализа и оценки рисков ИБ.