Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 07.11.2023 14:27:43
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ____02_____ 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Основы информационной безопасности»

Направление подготовки
**09.03.01 «Информатика и вычислительная техника»**

Профиль
**«Системная и программная инженерия»**

Квалификация
**Бакалавр**

Формы обучения
**Очная**

Москва, 2023 г.

**Разработчик(и):**

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Руководитель образовательной программы,  А.Ю. Гневшев

**Согласовано:**
Заведующий кафедрой «Инфокогнитивные технологии»,



ктн, доцент, / Е.А. Пухова /

# Содержание


1 Цели, задачи и планируемые результаты обучения по дисциплине ..... 4
2 Место дисциплины в структуре образовательной программы ..... 5
3 Структура и содержание дисциплины ..... 6
3.1 Виды учебной работы и трудоемкость ..... 6
3.2 Тематический план изучения дисциплины ..... 7
3.3 Содержание дисциплины ..... 8
3.4 Тематика семинарских/практических и лабораторных занятий ..... 9
3.5 Тематика курсовых проектов (курсовых работ) ..... 10
4 Учебно-методическое и информационное обеспечение ..... 10
4.1 Основная литература ..... 10
4.2 Дополнительная литература ..... 10
4.3 Электронные образовательные ресурсы ..... 11
4.4 Лицензионное и свободно распространяемое программное обеспечение ..... 11
5 Материально-техническое обеспечение ..... 11
6 Методические рекомендации ..... 12
6.1 Методические рекомендации для преподавателя по организации обучения ..... 12
6.2 Методические указания для обучающихся по освоению дисциплины ..... 12
7 Фонд оценочных средств ..... 12
7.1 Методы контроля и оценивания результатов обучения ..... 12
7.2 Шкала и критерии оценивания результатов обучения ..... 12
7.3 Оценочные средства ..... 17
7.3.1. Список вопросов для экзамена ..... 17

# 1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Основы информационной безопасности» следует отнести:

- раскрытие сущности и значения информационной безопасности и методов защиты информации в практических задачах и их место в системе национальной безопасности;
- формирование у студентов научного мировоззрения, понимания важности научно обоснованных методов для решения профессиональных задач в области безопасности информационных технологий.

К **основным задачам** освоения дисциплины «Основы информационной безопасности» следует отнести:

- овладение студентами понятийным аппаратом в области информационной безопасности и защиты информации; установление и раскрытие структуры угроз защищаемой информации;
- изучение базовых содержательных положений в области информационной безопасности и защиты информации; раскрытие современной доктрины информационной безопасности;
- раскрытие различных форм представления информации в проблемах обеспечения информационной безопасности.
- ознакомление с современными подходами к решению общей задачи – созданию комплексной(-ых) системы(-ем) защиты информации

Обучение по дисциплине **«Основы информационной безопасности»** направлено на формирование у обучающихся следующих компетенций:

| Код и наименование компетенций | Индикаторы достижения компетенции |
|---|---|
| ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения | ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД;<br>ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа. Настраивать параметры и сегментировать элементы администрируемой сети<br>ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа |

| | |
|---|---|
| | Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов). Документирование настроек средств обеспечения безопасности удаленного |
| ПК-3.Способен обслуживать сетевые устройства информационно-коммуникационной системы | ИПК-3.1. Знает: Базовую модель взаимодействия открытых систем для управления сетевым трафиком Международные стандарты ЛВС Процедуры и стандарты обновления ПО сетевых устройств, принятые в организации. Лицензионные требования по настройке обновляемого ПО сетевых устройств. Отраслевые нормативные правовые акты. Типы изменений в методологии инфраструктуры ИТ. Методы управления рисками Отчеты управляющей системы Локальные правовые акты, действующие в организации<br>ИПК-3.2. Умеет: Анализировать сообщения об ошибках в сетевых устройствах. Выявлять и устранять последствия сбоев и отказов сетевых устройств. Документировать изменения в конфигурации администрируемого ПО сетевых устройств. Обосновывать предложения по реализации стратегии в области ИКТ<br>ИПК-3.3. Владеет: Методами определения и выявления сбоев и отказов сетевых устройств и ОС. Сопоставлением аварийной информации от различных сетевых устройств ИКС. Локализацией отказов в сетевых устройствах Проверкой целостности ПО сетевых устройств ИКС. Загрузкой и выгрузкой (вручную или автоматически) в базу данных управляющей системы необходимых параметров |

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности», относится к числу профессиональных учебных дисциплин базовой части цикла Б.1.1 образовательной программы бакалавриата (Б.1.1.22) и взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: Организация ЭВМ и вычислительных систем; Проектирование и администрирование баз данных; Организационное и правовое обеспечение информационной безопасности, Методы и средств криптографической защиты информации.

# 3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, т.е. 108 академических часа (лекции - 8 часов, лабораторные занятия - 36 часов, самостоятельная работа – 64 часа, форма контроля - зачет) в 4 семестре.

## 3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

| № п/п | Вид учебной работы | Количество часов | Семестры | |
|---|---|---|---|---|
| | | | 4 | |
| **1** | **Аудиторные занятия** | **44** | 44 | |
| | В том числе: | | | |
| 1.1 | Лекции | 8 | 8 | |
| 1.2 | Семинарские/практические занятия | | | |
| 1.3 | Лабораторные занятия | 36 | 36 | |
| **2** | **Самостоятельная работа** | **64** | 64 | |
| **3** | **Промежуточная аттестация** | | | |
| | зачет | **зачет** | зачет | |
| | Итого: | **108** | 108 | |

## 3.2 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

| № п/п | Разделы/темы дисциплины | Трудоемкость, час | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | | | Самостоятельная работа |
| | | | Лекции | Семинарские/ практические занятия | Лабораторные занятия | Практическая подготовка | |
| 1 | **Тема 1.** Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности. | 1 | 1 | | 2 | | 4 |
| 2 | **Тема 2.** Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. | 11 | 3 | | 2 | | 4 |
| 3 | **Тема 3.** Информационная безопасность личности, общества и государства: социально-правовые аспекты | 10 | 2 | | 2 | | 4 |
| 4 | **Тема 4.** Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в компьютерных системах**.** | 15 | 2 | | 4 | | 6 |
| 5 | **Тема 5** Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации. | 14 | | | 4 | | 6 |
| 6 | **Тема 6.** Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации. | 10 | | | 2 | | 6 |
| 7 | **Тема 7.** Повышение эксплуатационной надежности КС. Защита информации в компьютерных системах от случайных угроз. | 11 | | | 2 | | 6 |
| 8 | **Тема 8.** Охрана объектов КС и средства защиты информации от утечки по техническим каналам. Противодействие подслушиванию. Методы и средства защиты КС от побочных электромагнитных излучений и наводок. | 16 | | | 2 | | 6 |
| 9 | **Тема 9.** Защита КС от несанкционированного вмешательства. Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам | 12 | | | 4 | | 4 |
| 10 | **Тема 10** Криптографические методы защиты информации. Основные понятия и методы шифрования**.** | 14 | | | 4 | | 6 |
| 11 | **Тема** 11 Компьютерные вирусы и средства антивирусной защиты. Общие сведения о компьютерных вирусах Профилактика заражения вирусами компьютерных систем | 14 | | | 4 | | 6 |
| 12 | **Тема 12** Комплексная защита информации в компьютерных системах (КСЗИ). Концепция | 14 | | | 4 | | 6 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | создания КСЗИ в КС. Функционирование КСЗИ. | | | | | | |
| **Итого** | | **108** | **8** | | **36** | | **64** |

## 3.3 Содержание дисциплины

Структура и содержание дисциплины «Основы информационной безопасности» по срокам и видам работы отражены в приложении.

**Первый семестр**

**Тема 1.** ***Введение.*** Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература.

**Тема 2.** ***Защита информации как объективная закономерность эволюции постиндустриального общества.*** Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Информационные технологии. Информационные ресурсы услуги. Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации. Правовое регулирование вопросов защиты информации.

**Тема 3.** ***Информационная безопасность личности, общества и государства: социально-правовые аспекты.*** Право на информацию в системе гражданских прав личности. Возможные ограничения. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Виды тайн. Коммерческая тайна. Государственная тайна. Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ. Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.

**Тема 4.** ***Угрозы информационной безопасности в компьютерных системах.*** Компьютерная система (КС) как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности.

**Тема 5.** ***Общая характеристика средств и методов защиты информации.*** Эволюция концепции информационной безопасности в компьютерных системах. Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя Обобщённые модели систем защиты информации. Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).

**Тема 6.** ***Организационно-правовое обеспечение защиты информации.*** Общая характеристика организационного обеспечения защиты информации. Основные задачи службы безопасности предприятия. Организационные мероприятия, обеспечивающие защиту информации. Необходимость правового регулирования в области защиты информации. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности; международные и отечественные нормативные и руководящие документы.

**Тема 7.** ***Защита информации в компьютерных системах от случайных угроз.*** Повышение эксплуатационной надежности КС. Сбои и отказы. Общие сведения о кодах для обнаружения и исправления случайных ошибок. Дублирование информации и резервирование

технических средств. Блокировка ошибочных операций. Минимизация ущерба от аварий и стихийных бедствий.

**Тема 8.** ***Охрана объектов КС и средства защиты информации от утечки по техническим каналам.*** Система охраны объектов КС. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Противодействие наблюдению в оптическом диапазоне. Противодействие подслушиванию. Методы и средства защиты от побочных электромагнитных излучений и наводок.

**Тема 9.** ***Защита компьютерных систем от несанкционированного вмешательства.*** Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования и исследования. Защита от несанкционированного изменения структуры КС в процессе эксплуатации. Контроль целостности программ и данных в процессе эксплуатации. Регистрация и контроль действий пользователей.

**Тема 10.** ***Криптографические методы защиты информации.*** Основные понятия и этапы развития криптографии. Классификация криптографических средств. Основные методы шифрования. Шифрование методами замены и перестановки. Аналитические и аддитивные методы шифрования. Системы шифрования с открытым ключом.

**Тема 11.** ***Компьютерные вирусы и средства антивирусной защиты.*** Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Механизмы заражения компьютерными вирусами. Методы и средства защиты от компьютерных вирусов. Профилактика заражения вирусами компьютерных систем

**Тема 12.** ***Комплексная защита информации в компьютерных системах.*** Концепция создания КСЗИ в КС. Технология разработки КСЗИ. Функционирование комплексных систем защиты информации. Аудит в защищенных КС. Организационная структура КСЗИ.

## 3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

*Не запланировано в учебном плане.*

3.4.2 Лабораторные занятия

*1. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе.*

*2. Информационная безопасность личности, общества и государства: социально-правовые аспекты*

*3. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в компьютерных системах.*

*4. Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации.*

*5. Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации*

*6. Повышение эксплуатационной надежности КС. Защита информации в компьютерных системах от случайных угроз.*

*7. Охрана объектов КС и средства защиты информации от утечки по техническим каналам. Противодействие подслушиванию. Методы и средства защиты КС от побочных электромагнитных излучений и наводок.*

*8. Защита КС от несанкционированного вмешательства. Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей, и разграничение их доступа к компьютерным ресурсам*

*9 Криптографические методы защиты информации. Основные понятия и методы шифрования.*

*10 Компьютерные вирусы и средства антивирусной защиты. Общие сведения о компьютерных вирусах Профилактика заражения вирусами компьютерных систем*

*11 Комплексная защита информации в компьютерных системах (КСЗИ). Концепция создания КСЗИ в КС. Функционирование КСЗИ.*

### 3.5 Тематика курсовых проектов (курсовых работ)

Не запланировано в учебном плане

## 4 Учебно-методическое и информационное обеспечение

### 4.1 Основная литература


1. Федоров Н.В. Основы информационной безопасности. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=561


### 4.2 Дополнительная литература


1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350.
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793
4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792
5. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
6. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее

образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368
7. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083
8. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933
9. Криптографические методы и средства защиты информации. Бутакова Н.Г., Федоров Н.В. - Санкт-Петербург: ИЦ "Интермедия", 2019
10. Рагозин Ю. Н. Инженерно-техническая защита информации: учебное пособие - Санкт-Петербург: ИЦ "Интермедия", 2018
11. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - 3-е издание Гриф УМО, 2012
12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. - М.: Горячая линия-Телеком, Гриф МО.
13. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432с.
14. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методические основы. МГИУ, 2009 - 367с.

### 4.3 Электронные образовательные ресурсы

1. Курс в лмс https://lms.mospolytech.ru/course/view.php?id=561
2. http://bibliotekar.ru/biznes-29/index.htm
3. http://citforum.ru/security/
4. http://www.itsec.ru/main.php
5. http://www.securrity.ru/
6. Локальный электронный учебник по направлению «Информационная безопасность» для бакалавров и специалистов. Федоров Н.В. Свидетельство о государственной регистрации программы для ЭВМ № 2013610300.

### 4.4 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Windows 7(или ниже) – Microsoft Open License. Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215.
2. Офисные приложения, Microsoft Office 2013(или ниже) – Microsoft Open License. Лицензия № 61984042.

## 5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

# 6 Методические рекомендации

## 6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

## 6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачёту, а также самостоятельно изучают отдельные темы учебной программы.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачете в письменной и устной форме.

# 7 Фонд оценочных средств

## 7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- устный опрос;
- проверка домашних заданий;
- экзамен.

## 7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

| **ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения**<br>**ПК-3. Способен обслуживать сетевые устройства информационно-коммуникационной системы** | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД;<br>ИПК-3.1. Знает: Базовую модель взаимодействия открытых систем для управления сетевым трафиком Международные стандарты ЛВС Процедуры и стандарты обновления ПО сетевых устройств, принятые в организации. Лицензионные требования по настройке обновляемого ПО сетевых устройств. Отраслевые нормативные правовые акты. Типы изменений в методологии инфраструктуры ИТ. | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации. | Обучающийся демонстрирует неполное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации | Обучающийся демонстрирует частичное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует полное соответствие следующих знаний: значение информации в развитии современного общества, информационные ресурсы, подлежащие защите, угрозы безопасности информации, свободно оперирует приобретенными знаниями. |

| | | | | |
|---|---|---|---|---|
| Методы управления рисками<br>Отчеты управляющей системы<br>Локальные правовые акты, действующие в организации | | | | |
| **ИПК-2.2. Уметь:**<br>Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа.<br>Настраивать параметры и сегментировать элементы администрируемой сети<br>ИПК-3.2. Умеет:<br>Анализировать сообщения об ошибках в сетевых устройствах.<br>Выявлять и устранять последствия сбоев и отказов сетевых устройств.<br>Документировать изменения в конфигурации администрируемого ПО сетевых устройств.<br>Обосновывать предложения по реализации стратегии в области ИКТ | Обучающийся не умеет или в недостаточной степени умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. | Обучающийся демонстрирует неполное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации. | Обучающийся демонстрирует частичное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | Обучающийся демонстрирует полное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |

| | | | | |
|---|---|---|---|---|
| **ИПК-2.3. Владеет:** Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов). Документирование настроек средств обеспечения безопасности удаленного ИПК-3.3. Владеет: Методами определения и выявления сбоев и отказов сетевых устройств и ОС. Сопоставлением аварийной информации от различных сетевых устройств ИКС. Локализацией отказов в сетевых устройствах Проверкой целостности ПО сетевых устройств ИКС. Загрузкой и | Обучающийся не владеет или в недостаточной степени владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. | Обучающийся владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях | Обучающийся частично владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | Обучающийся в полном объеме владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, свободно применяет полученные навыки в ситуациях повышенной сложности |

| | | | | |
|---|---|---|---|---|
| выгрузкой (вручную или автоматически) в базу данных управляющей системы необходимых параметров | | | | |

Шкалы оценивания результатов промежуточной аттестации и их описание:
***Форма промежуточной аттестации: зачет.***

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| **Шкала оценивания** | **Описание** |
|---|---|
| Отлично | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. |
| Удовлетворительно | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. |
| Неудовлетворительно | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

## 7.3 Оценочные средства

### 7.3.1. Список вопросов для экзамена

1. Основы Российского законодательства в области конфиденциальной информации.
2. Концепция IA*3.
3. Аудит информационной безопасности организации.
4. Внешний и внутренний аудит организации.
5. Конфиденциальная информация организации.
6. Криптографические методы защиты информации.
7. Персональные данные граждан.
8. Конфиденциальная информация банковской организации.
9. Общедоступные корпоративные информационные ресурсы.
10. Аудит конфиденциальных и персональных данных организации кредитно-финансовой системы РФ.
11. Стандарт безопасности Банка России.
12. Международный стандарт PCI DSS.
13. Специальные нормативные документы ФСТЭК.
14. Закон “О лицензировании отдельных видов деятельности” 99-ФЗ.
15. Закон “О персональных данных” 152-ФЗ.
16. ФЗ РФ от 29.07.2004 № 149-ФЗ О коммерческой тайне.
17. ФЗ РФ от 27 июля 2006 г. № 149-ФЗ Об информации, информационных технологиях и о защите информации.
18. ФЗ РФ от 27 декабря 2002 г. №184-ФЗ О техническом регулировании.