Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 04.09.2025 14:33:39
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"27" февраля 2025 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности»

Направление подготовки
**10.04.01 Информационная безопасность**

Профиль
**Системы управления информационной безопасностью**

Квалификация
**Магистр по защите информации**

Формы обучения
**Очная**

Москва, 2025 г.

**Разработчики:**
Доцент кафедры «Информационная безопасность», к.т.н, доцент:

 /А.Г.Спеваков /

**Согласовано:**
Заведующий кафедрой «Информационная безопасность»  /И.В.Калуцкий/

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

# 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 ..... 6
3.3 Содержание дисциплины ..... 7
3.4 Тематика семинарских/практических и лабораторных занятий ..... 8
4 Учебно-методическое и информационное обеспечение ..... 8
4.1. Нормативные документы и ГОСТы ..... 8
4.2. Основная литература ..... 8
4.3. Дополнительная литература ..... 9
4.5. Лицензионное и свободно распространяемое программное обеспечение ..... 9
4.6. Современные профессиональные базы данных и информационные справочные системы ..... 9
5. Материально-техническое обеспечение ..... 9
6. Методические рекомендации ..... 10
6.1. Методические рекомендации для преподавателя по организации обучения ..... 10
6.2. Методические указания для обучающихся по освоению дисциплины ..... 10
7. Фонд оценочных средств ..... 11
7.1. Методы контроля и оценивания результатов обучения ..... 11
7.2. Шкала и критерии оценивания результатов обучения ..... 11
7.3. Оценочные средства ..... 12

# 1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» следует отнести:

- обучение навыкам разработки проектов организационно-распорядительной документации по обеспечению информационной безопасности;
- получение студентами знаний об обязательных разделах ОРД;
- формирование практических навыков в области аттестации объектов информатизации по требованиям безопасности информации;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистратуры по направлению, в том числе формирование у них умений по организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

К **основным задачам** освоения дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» следует отнести:

- Приобретение знаний о методах разработки организационно-распорядительных документов по обеспечению информационной безопасности.
- Овладение знаниями о возможностях технических средств перехвата информации;
- Приобретение знаний о правовых нормативных актах и нормативных методических документов ФСБ России, ФСТЭК России.
- Приобретение навыков обобщения, оценивания и анализа результатов, в ходе исследований в области защиты информации.
- Овладение принципами проведения экспериментально-исследовательских работ при аттестации объектов информатизации с учетом нормативных документов по защите информации.
- Освоение методов организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности.

В результате освоения дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

| Код и наименование компетенций | Индикаторы достижения компетенции |
|---|---|
| ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности | **знать:**<br>требования по оформлению технической документации в соответствии с Единой системы конструкторской документации и Единой системы программной документации<br>**уметь:**<br>разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.<br>**владеть:**<br>навыками разработки основных разделов ОРД |
| ПК-10. Способен проводить аттестацию объектов информатизации по требованиям безопасности информации | **знать:**<br>возможности технических средств перехвата информации.<br>**уметь:** |

| | |
|---|---|
| | проводить экспериментально-исследовательские работы при аттестации объектов информатизации с учетом нормативных документов по защите информации.<br>**владеть:**<br>навыками проведения экспериментально-исследовательских работ при аттестации объектов информатизации с учетом нормативных документов по защите информации. |
| ПК-14. Способен организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России | **знать:**<br>правовые нормативные актами и нормативными методическими документами ФСБ России, ФСТЭК России.<br>**уметь:**<br>организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности.<br>**владеть:**<br>навыками управления организации работ по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности. |
| ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности | **знать:**<br>методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности.<br>**уметь:**<br>организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.<br>**владеть:**<br>методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. |

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» относится к числу обязательных профессиональных учебных дисциплин, цикла (Б1.1) основной образовательной программы магистра (Б1.1.6).

Дисциплина «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности» и «Построение и совершенствование систем управления информационной безопасностью».

Дисциплина обеспечивает изучение дисциплин «Стратегии управления информационной безопасностью» и подготовку выпускной квалификационной работы.

# 3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, т.е. **108** академических часа (лекции – 18 часов, лабораторные занятия – 36 часа, самостоятельная работа студентов – 54 часа, форма контроля – экзамен) во 2 семестре.

Структура и содержание дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» по срокам и видам работы отражены в приложении.

## 3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

| № п/п | Вид учебной работы | Количество часов | Семестры | |
|---|---|---|---|---|
| | | | 2 | |
| **1** | **Аудиторные занятия** | **54** | 54 | |
| | В том числе: | | | |
| 1.1 | Лекции | 18 | 18 | |
| 1.2 | Семинарские/практические занятия | - | - | |
| 1.3 | Лабораторные занятия | 36 | 36 | |
| **2** | **Самостоятельная работа** | **54** | 54 | |
| 2.1 | СРС | | | |
| **3** | **Промежуточная аттестация** | | | |
| | Зачет/диф. зачет/экзамен | | Экзамен | |
| | Курсовой проект | | - | |
| | **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 | |
| 1.1 | Тема 1. Политика идентификации и аутентификации | 6 | 2 | - | 2 | - | 2 |
| 1.2 | Тема 2. Политика управления доступом | 6 | 2 | - | 2 | - | 4 |
| 1.3 | Тема 3. Политика ограничения программной среды | 6 | - | - | 2 | - | 2 |
| 1.4 | Тема 4. Политика защиты машинных носителей | 6 | - | - | 2 | - | 4 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.5 | Тема 5. Политика аудита безопасности | 8 | 2 | - | 4 | - | 4 |
| 1.6 | Тема 6. Политика антивирусной защиты | 6 | 2 | | 4 | | 4 |
| 1.7 | Тема 7. Политика предотвращения вторжений | 8 | - | | 4 | | 4 |
| 1.8 | Тема 8. Политика обеспечения целостности и доступности | 6 | 2 | | 2 | | 2 |
| 1.9 | Тема 9. Политика защиты технических средств и систем | 8 | - | | 2 | | 4 |
| 1.10 | Тема 10. Политика реагирования на компьютерные инциденты | 8 | 2 | | 2 | | 4 |
| 1.11 | Тема 11. Политика управления конфигурацией информационной системой | 8 | 2 | | 2 | | 4 |
| 1.12 | Тема 12. Технический паспорт | 8 | - | | 2 | | 4 |
| 1.13 | Тема 13. Политика планирования мероприятий по обеспечению защиты информации | 8 | 2 | | 2 | | 4 |
| 1.14 | Тема 14. Политика обеспечения действий в нештатных ситуациях | 8 | 2 | | 2 | | 4 |
| 1.15 | Тема 15. Политика информирования и обучения персонала | 8 | - | | 2 | | 4 |
| **Итого** | | **108** | **18** | | **36** | | **54** |

## 3.3 Содержание дисциплины

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Раздел 1 | |
| 1.1 | Тема 1. Политика идентификации и аутентификации | Методы и алгоритмы идентификации и аутентификации. Навыки разработки политики. |
| 1.2 | Тема 2. Политика управления доступом | Методы и алгоритмы управления доступом. Матрицы доступа. Навыки разработки политики. |
| 1.3 | Тема 3. Политика ограничения программной среды | Методы и средства ограничения программной среды. Навыки разработки политики. |
| 1.4 | Тема 4. Политика защиты машинных носителей | Методы и средства защиты машинных носителей. Навыки разработки политики. |
| 1.5 | Тема 5. Политика аудита безопасности | Методы аудита информационной безопасности. Навыки разработки политики. |
| 1.6 | Тема 6. Политика антивирусной защиты | Методы и средства антивирусной защиты. Навыки разработки политики. |

| № п/п | Раздел (тема) дисциплины | Содержание |
|---|---|---|
| 1.7 | Тема 7. Политика предотвращения вторжений | Методы и алгоритмы предотвращения вторжений. Навыки разработки политики. |
| 1.8 | Тема 8. Политика обеспечения целостности и доступности | Методы и алгоритмы обеспечения целостности и доступности. Навыки разработки политики. |
| 1.9 | Тема 9. Политика защиты технических средств и систем | Методы и средства защиты технических средств и систем. Навыки разработки политики. |
| 1.10 | Тема 10. Политика реагирования на компьютерные инциденты | Анализ компьютерных инцидентов, методы и средства реагирования. Навыки разработки политики. |
| 1.11 | Тема 11. Политика управления конфигурацией информационной системой | Методы и средства управления конфигурацией информационной системой. Навыки разработки политики. |
| 1.12 | Тема 12. Технический паспорт | Приказы ФСТЭК. Технический паспорт информационной системы. Технический паспорт помещения. |
| 1.13 | Тема 13. Политика планирования мероприятий по обеспечению защиты информации | Методы и регламенты планирования мероприятий по обеспечению защиты информации. Навыки разработки политики. |
| 1.14 | Тема 14. Политика обеспечения действий в нештатных ситуациях | Методы и регламенты обеспечения действий в нештатных ситуациях. Навыки разработки политики. |
| 1.15 | Тема 15. Политика информирования и обучения персонала | Методы и регламенты информирования и обучения персонала. Навыки разработки политики. |

## 3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные занятия

**Лабораторная работа 1.** Разработка политики идентификации и аутентификации
**Лабораторная работа 2.** Разработка политики управления доступом
**Лабораторная работа 3**. Разработка политики ограничения программной среды
**Лабораторная работа 4**. Разработка политики защиты машинных носителей
**Лабораторная работа 5.** Разработка политики аудита безопасности
**Лабораторная работа 6.** Разработка политики антивирусной защиты
**Лабораторная работа 7.** Разработка политики предотвращения вторжений
**Лабораторная работа 8.** Разработка политики обеспечения целостности и доступности
**Лабораторная работа 9.** Разработка политики защиты технических средств и систем
**Лабораторная работа 10.** Разработка политики реагирования на компьютерные инциденты

**Лабораторная работа 11.** Разработка политики управления конфигурацией информационной системой

**Лабораторная работа 12.** Технический паспорт

**Лабораторная работа 13**. Разработка политики планирования мероприятий по обеспечению защиты информации

**Лабораторная работа 14.** Разработка политики обеспечения действий в нештатных ситуациях

**Лабораторная работа 15.** Разработка политики информирования и обучения персонала

# 4 Учебно-методическое и информационное обеспечение

## 4.1. Нормативные документы и ГОСТы

1 ГОСТ Р 7.0.97-2016 Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов. https://protect.gost.ru/document.aspx?control=7&id=205885

2 Приказ ФСТЭК России от 25 декабря 2017 г. N 239 https://fstec.ru/files/212/----25--2017--N-239/217/----25--2017--N-239.pdf

3 Приказ ФСТЭК России от 21 декабря 2017 г. N 235 https://fstec.ru/files/214/----21--2017--N-235/221/----21--2017--N-235.pdf

## 4.2. Основная литература


1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.
2. Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172840 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.
3. Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182279 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.


## 4.3. Дополнительная литература


1. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.

2. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.
3. Зубо, С. А. Data Security : учебно-методическое пособие / С. А. Зубо, Е. А. Филатова, И. В. Бакатович. — Москва : РТУ МИРЭА, 2022. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256607 (дата обращения: 10.02.2023). — Режим доступа: для авториз. пользователей.

### 4.4. Электронные образовательные ресурсы

1. Электронный образовательный ресурс на стадии разработки.

### 4.5. Лицензионное и свободно распространяемое программное обеспечение

Libreoffice бесплатное ПО, Ubuntu 22.04 LTS бесплатное ПО.

### 4.6. Современные профессиональные базы данных и информационные справочные системы

1. Банк данных угроз безопасности информации https://bdu.fstec.ru/

## 5. Материально-техническое обеспечение

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

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки магистр 10.04.01 Информационная безопасность.

### 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 и практической подготовки студентов являются лекции и лабораторные работы.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторном занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на лабораторных занятиях, промежуточный контроль осуществляется в тестовой форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в устной форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений;
- оформление материала в соответствии с требованиями.

## 7. Фонд оценочных средств

## 7.1. Методы контроля и оценивания результатов обучения

Методика преподавания дисциплины «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

- защита лабораторных работ;
- подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;
- использование интерактивных форм текущего контроля в форме тестирования;

## 7.2. Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
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 Текущий контроль

Оценочные средства для текущей аттестации

- Защита отчетов о выполнении лабораторных работ

7.3.2. Промежуточная аттестация

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».

**Вопросы к экзамену по дисциплине**

1. Выбор задач и средств защиты информации.
2. Задачи защиты содержания информации.
3. Задачи уменьшения степени распознавания объектов
4. Категорирование помещений. Порядок сдачи и приема объекта под охрану.
5. Классификационная структура подходов к проектированию СЗИ. Обобщенный алгоритм проектирования СЗИ.
6. Классификация возможных угроз информации по видам, характеру происхождения, источникам, предпосылкам появления и взаимодействию.
7. Классификация каналов несанкционированного получения информации. Модель канала утечки информации.
8. Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации.
9. Моделирование систем и процессов защиты информации. Обобщенная модель процессов защиты информации. Модель нарушителя по ГТК.
10. Моделирование систем и процессов защиты информации. Общая модель СЗИ.
11. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения
12. Определение требований к защите информации. Требования по заданию уровня защищенности информации.
13. Организационное построение СЗИ. Семирубежная модель.
14. Организационно-правовое и документальное обеспечение защиты информации.
15. Организация и обеспечение работ по защите информации. Определение требований к СЗИ.
16. Организация и обеспечение работ по защите информации. Проектирование, создание и эксплуатация СЗИ.
17. Организация и обеспечение работ по защите информации. Управление процессами функционирования СЗИ. Общая модель управления защитой.
18. Организация и обеспечение работ по защите информации. Управление процессами функционирования СЗИ. Планирование и оперативное управление.
19. Организация и обеспечение работ по защите информации. Управление процессами функционирования СЗИ. Календарно-плановое руководство.
20. Организация и обеспечение работ по защите информации. Установление мер контроля и ответственности.

21. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима

22. Оценка безопасности информации на объектах обработки. Обобщенный подход.

23. Оценка безопасности информации на объектах обработки. Определение показателей защищенности информации.

24. Оценка безопасности информации на объектах обработки.

25. Оценка безопасности информации на объектах обработки. Рекомендации по использованию моделей.

26. Оценка безопасности информации на объектах обработки. Теоретико-эмпирический подход. Модель оценки по уровню безопасности информации.

27. Оценка безопасности информации на объектах обработки. Теоретико-эмпирический подход. Модель оценки на основе теории игр.

28. Оценка безопасности информации на объектах обработки. Теоретический подход.

29. Оценка безопасности информации на объектах обработки. Эмпирический подход.

30. Показатели, используемые для оценки информации

31. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации

32. Проектирование систем защиты информации. Алгоритм проектирования индивидуальных СЗИ.

33. Проектирование систем защиты информации. Обобщенная структура показателей оптимальности построения СЗИ.

34. Цели и задачи охраны. Объекты охраны. Виды и способы охраны. Посты охраны, связь, взаимодействие с местными органами правопорядка

35. Требования к помещениям, в которых циркулирует защищаемая информация

36. Средства и методы физической защиты объектов

37. Способы и средства защиты информации

38. Стратегии защиты информации

39. Структура информационной безопасности.

40. Структура информационной безопасности. Направления Российской системы информационной безопасности.

41. Структурная схема СЗИ. Организационно-правовое обеспечение. Ресурсы информационно-вычислительной системы.

42. Требования к архитектуре системы защиты информации. Принципы построения системы защиты информации.

43. Технические средства охраны и видеонаблюдения объекта

44. Функциональное построение системы защиты информации. Криптографическая подсистема.

45. Функциональное построение системы защиты информации. Подсистема обеспечения целостности.

46. Функциональное построение системы защиты информации. Подсистема ограничения доступа.

47. Функциональное построение системы защиты информации. Подсистема регистрации и учета.

48. Функциональное построение системы защиты информации. Подсистема управления.

49. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.

**Пример билета по курсу**
**«Проектирование организационно-распорядительных документов по обеспечению информационной безопасности»**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности»
Магистры. Курс 1, семестр 2

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Оценка безопасности информации на объектах обработки.
2. Стратегии защиты информации

Преподаватель _____ / Спеваков А.Г. /