

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение  
высшего образования  
**«Российский государственный гуманитарный университет»**  
**(ФГАОУ ВО «РГГУ»)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ  
Кафедра комплексной защиты информации

**ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ  
В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

*Код и наименование направления подготовки/специальности*

«Безопасность автоматизированных систем

(по отрасли или в сфере профессиональной деятельности)»

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2026

*Защита от несанкционированного доступа к информации в автоматизированных системах*  
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент, зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры  
комплексной защиты информации  
№ 5 от 25.12.2025

## ОГЛАВЛЕНИЕ

|   |    |
|---|----|
| 1. Пояснительная записка .....  | 4  |
| 1.1. Цель и задачи дисциплины .....   | 4  |
| 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций .....          | 4  |
| 1.3. Место дисциплины в структуре образовательной программы .....   | 5  |
| 2. Структура дисциплины .....   | 5  |
| 3. Содержание дисциплины .....  | 5  |
| 4. Образовательные технологии .....   | 7  |
| 5. Оценка планируемых результатов обучения .....  | 8  |
| 5.1 Система оценивания .....  | 8  |
| 5.2 Критерии выставления оценки по дисциплине .....   | 9  |
| 5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине ..... | 10 |
| 6. Учебно-методическое и информационное обеспечение дисциплины .....  | 12 |
| 6.1 Список источников и литературы .....  | 12 |
| 6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» .....  | 15 |
| 6.3 Профессиональные базы данных и информационно-справочные системы .....   | 15 |
| 7. Материально-техническое обеспечение дисциплины .....   | 15 |
| 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов .....                       | 16 |
| 9. Методические материалы .....   | 17 |
| 9.1 Планы практических занятий .....  | 17 |
| Приложение 1. Аннотация рабочей программы дисциплины .....  | 19 |

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины – получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от несанкционированного доступа (НСД); формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.

Задачи дисциплины:

- овладение методами решения профессиональных задач по защите информации от НСД;
- формирование навыков работы с современными средствами защиты информации от НСД.

### 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

| Компетенция<br>(код и наименование)   | Индикаторы компетенций<br>(код и наименование)  | Результаты обучения   |
|---|---|---|
| ПК-13<br>Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации | ПК-13.1<br>Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации | Знать: <ul style="list-style-type: none"> <li>• процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации;</li> </ul>                    |
|   | ПК-13.2<br>Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации   | Владеть: <ul style="list-style-type: none"> <li>• навыками организации процесса аттестации объектов вычислительной техники и выделенных помещений;</li> <li>• навыками сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации сетей</li> </ul> |
|   | ПК-13.3<br>Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации   | Уметь: <ul style="list-style-type: none"> <li>• разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации</li> </ul>   |
| ПК-8<br>Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах  | ПК-8.1<br>Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации  | Знать: <ul style="list-style-type: none"> <li>• основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;</li> <li>• организационные меры по защите информации;</li> </ul>   |
|   | ПК-8.2<br>Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов  | Уметь: <ul style="list-style-type: none"> <li>• анализировать программные, архитектурно-технические и схемотехнические решения компонентов</li> </ul>   |

|  |  |   |
|--|--|---|
|  | автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем | автоматизированных систем;<br><ul style="list-style-type: none"> <li>• выявлять потенциальные уязвимости безопасности информации в автоматизированных системах;</li> <li>• вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем</li> </ul> |
|  | ПК-8.3<br>Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы   | Владеть:<br><ul style="list-style-type: none"> <li>• навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы</li> </ul>  |

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита от несанкционированного доступа к информации в автоматизированных системах» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

## 2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

### Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий      | Количество часов |
|---------|--------------------------|------------------|
| 5       | Лекции                   | 28               |
| 5       | Практические работы      | 32               |
| 5       | Промежуточная аттестация | 18               |
| Всего:  |                          | 64               |

Объем дисциплины в форме самостоятельной работы обучающихся составляет 26 академических часов.

## 3. Содержание дисциплины

### *Тема 1. Введение в защиту информации от несанкционированного доступа*

Основные термины и определения ЗИ от НСД. Классификация требований к системам защиты от НСД. Ответственность за НСД. Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов, стандартов, руководящих документов и требований по ЗИ от НСД. Особенности современных АС. Виды угроз современным АС. Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.

### *Тема 2. Требования к защите информации от несанкционированного доступа*

Формализованные требования к ЗИ от НСД. Классы защищённости СВТ. Классификация АС по защищённости от НСД. Состав первой группы защиты АС. Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.

### *Тема 3. Методы идентификации и аутентификации пользователя*

Понятие идентификации и аутентификации. Процедура авторизации. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. Классификация задач, решаемых механизмами идентификации и аутентификации. Критерии классификации. Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты. Угрозы преодоления парольной защиты. Явные и скрытые угрозы. Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля. Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация. Протоколы аутентификации.

#### ***Тема 4. Управление доступом к ресурсам***

Основные способы разделения доступа субъектов к совместно используемым объектам. Абстрактные модели доступа. Модели Биба, Гогена-Мезигера, Кларка-Вильсона, Сазерлендская модель. Дискреционная (матричная) модель. Многоуровневые (мандатные) модели. Понятия «владелец» и «собственник» информации.

Базовые модели доступа. Дискреционное разграничение доступа. Матрица доступа и домен безопасности. Список прав доступа ACL. Мандатное разграничение доступа. Ролевая модель разграничения доступа. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.

Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом. Централизованное и децентрализованное управление доступом. Протоколы аутентификации (AAA). RADIUS, TACACS.

#### ***Тема 5. Разработка политики безопасности информационной системы***

Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности. Важные аспекты при разработке политик безопасности. Средства защиты информации для государственных и коммерческих структур. Процесс разработки политики безопасности. Примерный состав группы по разработке политик безопасности. Требования к политикам безопасности. Типовые политики безопасности.

Реализация политик безопасности. Общие правила безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.

#### ***Тема 6. Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности***

Типовая методика анализа защищённости ИС. Методы тестирования систем информационной безопасности. Методы количественной оценки систем информационной безопасности. Методы и средства анализа защищённости автоматизированной системы. Анализ защищённости внешнего периметра корпоративной сети. Анализ защищённости внутренней инфраструктуры сети. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.

#### ***Тема 7. Применение средств аппаратной защиты***

Необходимость и принципы использования аппаратных средств защиты. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты. Метод контроля вскрытия аппаратуры, общий подход. Реализация си-

стемы контроля вскрытия аппаратуры. Принципы комплексирования средств защиты информации

#### 4. Образовательные технологии

| № п/п | Наименование раздела   | Виды учебных занятий                    | Образовательные технологии  |
|-------|--|---|---|
| 1     | 2  | 3                                       | 4   |
| 1.    | Введение в защиту информации от несанкционированного доступа                                       | Лекция 1.<br><br>Самостоятельная работа | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 2     | Требования к защите информации от несанкционированного доступа                                     | Лекция 2.<br><br>Самостоятельная работа | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 3     | Авторизация. Методы идентификации и аутентификации пользователя                                    | Лекция 3.<br><br>Самостоятельная работа | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 4     | Управление доступом к ресурсам   | Лекция 4.<br><br>Самостоятельная работа | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 5     | Разработка политики безопасности информационной системы  | Лекция 5<br><br>Самостоятельная работа  | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 6     | Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности | Лекция 6<br><br>Самостоятельная работа  | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 7     | Применение средств аппаратной защиты   | Лекция 7<br><br>Самостоятельная работа  | Традиционная лекция с использованием презентаций, опрос<br><br>Подготовка к занятиям с использованием ЭБС |
| 8     | Анализ источников, каналов распространения и каналов утечки информации                             | Практическое занятие 1                  | Выполнение и защита практической работы   |
| 9     | Запуск и регистрация в системе защиты  | Практическое занятие 2                  | Выполнение и защита практической работы   |
| 10    | Реализация дискреционной модели разграничения доступа  | Практическое занятие 3                  | Выполнение и защита практической работы   |

|    |   |                        |   |
|----|---|------------------------|---|
| 11 | Контроль целостности                              | Практическое занятие 4 | Выполнение и защита практической работы |
| 12 | Гарантированное удаление данных                   | Практическое занятие 5 | Выполнение и защита практической работы |
| 13 | Реализация мандатной модели разграничения доступа | Практическое занятие 6 | Выполнение и защита практической работы |

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

## 5. Оценка планируемых результатов обучения

### 5.1 Система оценивания

| Форма контроля  | Макс. количество баллов |                   |
|---|-------------------------|-------------------|
|   | За одну работу          | Всего             |
| Текущий контроль:                                       |                         |                   |
| - опрос   | 8 баллов                | 48 баллов         |
| - практическое занятие 1-6                              | 2 балла                 | 12 баллов         |
| Промежуточная аттестация – экзамен (экзамен по билетам) |                         | 40 баллов         |
| <b>Итого за семестр</b>                                 |                         | <b>100 баллов</b> |

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

| 100-балльная шкала | Традиционная шкала  |            | Шкала ECTS |
|--------------------|---------------------|------------|------------|
| 95 – 100           | отлично             | зачтено    | A          |
| 83 – 94            |                     |            | B          |
| 68 – 82            | хорошо              |            | C          |
| 56 – 67            | удовлетворительно   |            | D          |
| 50 – 55            |                     |            | E          |
| 20 – 49            | неудовлетворительно | не зачтено | FX         |
| 0 – 19             |                     |            | F          |

## 5.2 Критерии выставления оценки по дисциплине

| Баллы/<br>Шкала<br>ECTS | Оценка по<br>дисциплине | Критерии оценки результатов обучения по дисциплине  |
|-------------------------|-------------------------|---|
| 100-83/<br>A,B          | отлично                 | <p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>                                   |
| 82-68/<br>C             | хорошо                  | <p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>                                       |
| 67-50/<br>D,E           | удовлетворительно       | <p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p> |
| 49-0/<br>F,FX           | неудовлетворительно     | <p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>               |

## 5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

### *Устный опрос*

**Устный опрос** – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

**Перечень устных вопросов для проверки знаний**

| №   | Вопрос  | Реализуемая компетенция |
|-----|---|-------------------------|
| 1.  | Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.   | ПК-8, ПК-13             |
| 2.  | Виды угроз современным АС.  | ПК-8, ПК-13             |
| 3.  | Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.  | ПК-8, ПК-13             |
| 4.  | Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.  | ПК-8, ПК-13             |
| 5.  | Понятие идентификации и аутентификации. Процедура авторизации.  | ПК-8, ПК-13             |
| 6.  | Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. | ПК-8, ПК-13             |
| 7.  | Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.   | ПК-8, ПК-13             |
| 8.  | Угрозы преодоления парольной защиты.  | ПК-8, ПК-13             |
| 9.  | Основные механизмы ввода пароля.  | ПК-8, ПК-13             |
| 10. | Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.   | ПК-8, ПК-13             |
| 11. | Протоколы аутентификации.   | ПК-8, ПК-13             |
| 12. | Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.  | ПК-8, ПК-13             |
| 13. | Дискреционное разграничение доступа.  | ПК-8, ПК-13             |
| 14. | Мандатное разграничение доступа.  | ПК-8, ПК-13             |
| 15. | Ролевая модель разграничения доступа.   | ПК-8, ПК-13             |
| 16. | Управления доступом на основе атрибутов. Выбор модели разграничения доступа.  | ПК-8, ПК-13             |
| 17. | Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.  | ПК-8, ПК-13             |
| 18. | Централизованное и децентрализованное управление доступом.  | ПК-8, ПК-13             |
| 19. | Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.  | ПК-8, ПК-13             |
| 20. | Процесс разработки политики безопасности. Требования к политикам безопасности.  | ПК-8, ПК-13             |
| 21. | Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.   | ПК-8, ПК-13             |
| 22. | Типовая методика анализа защищённости ИС  | ПК-8, ПК-13             |
| 23. | Методы количественной оценки систем информационной безопасности.  | ПК-8, ПК-13             |
| 24. | Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.  | ПК-8, ПК-13             |
| 25. | Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.  | ПК-8, ПК-13             |
| 26. | Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.  | ПК-8, ПК-13             |
| 27. | Реализация программно-аппаратного контроля (мониторинга) активно-   | ПК-8, ПК-13             |

|     |  |             |
|-----|--|-------------|
|     | сти системы защиты.  |             |
| 28. | Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.      | ПК-8, ПК-13 |
| 29. | Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты. | ПК-8, ПК-13 |
| 30. | Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.                   | ПК-8, ПК-13 |
| 31. | Принципы комплексирования средств защиты информации  | ПК-8, ПК-13 |
| 32. | Угрозы перевода системы защиты в пассивное состояние, их реализация.   | ПК-8, ПК-13 |
| 33. | Метод контроля вскрытия аппаратуры, общий подход.  | ПК-8, ПК-13 |
| 34. | Принципы комплексирования средств защиты информации  | ПК-8, ПК-13 |

**Промежуточная аттестация (примерные вопросы к экзамену)**

| №   | Вопрос  | Реализуемая компетенция |
|-----|---|-------------------------|
| 1.  | Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.   | ПК-8, ПК-13             |
| 2.  | Виды угроз современным АС.  | ПК-8, ПК-13             |
| 3.  | Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.  | ПК-8, ПК-13             |
| 4.  | Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.  | ПК-8, ПК-13             |
| 5.  | Понятие идентификации и аутентификации. Процедура авторизации.  | ПК-8, ПК-13             |
| 6.  | Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. | ПК-8, ПК-13             |
| 7.  | Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.   | ПК-8, ПК-13             |
| 8.  | Угрозы преодоления парольной защиты.  | ПК-8, ПК-13             |
| 9.  | Основные механизмы ввода пароля.  | ПК-8, ПК-13             |
| 10. | Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.   | ПК-8, ПК-13             |
| 11. | Протоколы аутентификации.   | ПК-8, ПК-13             |
| 12. | Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.  | ПК-8, ПК-13             |
| 13. | Дискреционное разграничение доступа.  | ПК-8, ПК-13             |
| 14. | Мандатное разграничение доступа.  | ПК-8, ПК-13             |
| 15. | Ролевая модель разграничения доступа.   | ПК-8, ПК-13             |
| 16. | Управления доступом на основе атрибутов. Выбор модели разграничения доступа.  | ПК-8, ПК-13             |
| 17. | Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.  | ПК-8, ПК-13             |
| 18. | Централизованное и децентрализованное управление доступом.  | ПК-8, ПК-13             |
| 19. | Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.  | ПК-8, ПК-13             |
| 20. | Процесс разработки политики безопасности. Требования к политикам безопасности.  | ПК-8, ПК-13             |
| 21. | Реализация политик безопасности. Архитектура корпоративной системы  | ПК-8, ПК-13             |

|     |  |             |
|-----|--|-------------|
|     | защиты информации. Настройки основных компонент системы защиты компании.   |             |
| 22. | Типовая методика анализа защищённости ИС   | ПК-8, ПК-13 |
| 23. | Методы количественной оценки систем информационной безопасности.   | ПК-8, ПК-13 |
| 24. | Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.   | ПК-8, ПК-13 |
| 25. | Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.   | ПК-8, ПК-13 |
| 26. | Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние. | ПК-8, ПК-13 |
| 27. | Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.  | ПК-8, ПК-13 |
| 28. | Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.                                    | ПК-8, ПК-13 |
| 29. | Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.                               | ПК-8, ПК-13 |
| 30. | Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.   | ПК-8, ПК-13 |
| 31. | Принципы комплексирования средств защиты информации  | ПК-8, ПК-13 |

### *Примерные тестовые задания*

- 1) Диспетчер доступа характерен для
- а) ролевой модели разграничения доступа
  - б) мандатной модели разграничения доступа
  - в) дискреционной модели разграничения доступа

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Список источников и литературы**

#### Источники

#### Основные

1. *Руководящий документ*. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/485/---30--1992-398/872/--30--1992-.pdf>, свободный. – Загл. с экрана.
2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/487/---30--1992-400/876/---30--1992-.pdf>, свободный. – Загл. с экрана.
3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/486/---30--1992-399/874/---30--1992-.pdf>, свободный. – Загл. с экрана.
4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной

- технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/488/---25--1997-401/878/---25--1997-.pdf>, свободный. – Загл. с экрана.
5. *Руководящий документ*. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114 [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/489/---4--1999--N-114/880/---4--1999--N-114.pdf> свободный. – Загл. с экрана.
  6. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/492/---15--2008-/887/---15--2008-.pdf>, свободный. – Загл. с экрана.
  7. *Федеральный закон «Об информации, информационных технологиях и о защите информации»* от 27.07.2006 N 149-ФЗ. [Электронный ресурс] : Режим доступа : [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/), свободный. – Загл. с экрана.
- Дополнительные
8. *Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»* [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/), свободный. – Загл. с экрана.
  9. *Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»* [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_40241/](https://www.consultant.ru/document/cons_doc_LAW_40241/), свободный. – Загл. с экрана.
  10. *Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности»* [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_113658/](https://www.consultant.ru/document/cons_doc_LAW_113658/), свободный. – Загл. с экрана.
  11. *Федеральный закон от 30 декабря 2001 г. N 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях»*. [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/](https://www.consultant.ru/document/cons_doc_LAW_34661/), свободный. – Загл. с экрана.
  12. *Указ Президента Российской Федерации от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»*. [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_14031/](https://www.consultant.ru/document/cons_doc_LAW_14031/), свободный. – Загл. с экрана.
  13. *Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»*. [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_13532/](https://www.consultant.ru/document/cons_doc_LAW_13532/), свободный. – Загл. с экрана.
  14. *Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»*. [Электронный ресурс] : Режим доступа : [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_75586/](https://www.consultant.ru/document/cons_doc_LAW_75586/), свободный. – Загл. с экрана.
  15. *Положение о сертификации средств защиты информации*. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/568/-----26--1995--N-608/1024/-----26--1995--N-608.pdf>, свободный. – Загл. с экрана.
  16. *Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных*. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. N 21. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/234/----18--2013--N-21/262/----18--2013--N-21.pdf>, свободный. – Загл. с экрана.

17. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/files/493/---11--2014-/888/---11--2014-.pdf>, свободный. – Загл. с экрана.
18. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>, свободный. – Загл. с экрана.
19. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. No 416/489. ) [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-31-avgusta-2010-g-n-489>, свободный. – Загл. с экрана.

### Литература

#### Основная

1. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник для вузов / М. В. Тумбинская, М. В. Петровский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2025. — 344 с. — ISBN 978-5-507-52270-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/445253>. — Режим доступа: для авториз. пользователей.
2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7970-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/169817>. — Режим доступа: для авториз. пользователей.
3. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. – Москва : Гор. линия-Телеком, 2016. – 248 с. (Специальность) ISBN 978-5-9912-0470-5. – Текст : электронный. – URL: <https://znanium.com/catalog/product/973806>. – Режим доступа: по подписке.
4. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2025. — 337 с. — (Высшее образование). — DOI 10.12737/1932260. - ISBN 978-5-16-018225-4. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2199796>. – Режим доступа: по подписке..

#### Дополнительная

5. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2025. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2206781>. – Режим доступа: по подписке.
6. *Битнер, В. И.* Сети нового поколения - NGN: Учебное пособие для вузов / В.И. Битнер, Ц.Ц. Михайлова. – Москва : Гор. линия-Телеком, 2011. - 226 с.: ил.; . – (Специальность). ISBN 978-5-9912-0149-0, 500 экз. – Текст : электронный. – URL: <https://znanium.com/catalog/product/308917> . – Режим доступа: по подписке.

### **6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)
2. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
3. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)
4. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)

5. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
6. ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)
7. Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)
8. Электронная библиотека Grebennikon.ru [www.grebennikon.ru](http://www.grebennikon.ru)

### **6.3 Профессиональные базы данных и информационно-справочные системы**

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

## **7. Материально-техническое обеспечение дисциплины**

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

- 2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Cisco Packet Tracer v.7.2
6. Apache 2.0
7. Nginx
8. WireShark

## **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA SE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1 Планы практических занятий**

**Темы** учебной дисциплины предусматривают проведение практических работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических работ, выдаваемые преподавателем на каждом занятии.

**Целью** практических работ является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

**Тематика** практических работ соответствует программе дисциплины.

### ***Практическая работа 1 (4 ч.) Анализ источников, каналов распространения и каналов утечки информации***

Задания:

- Исследовать осциллограммы и спектры получаемых сигналов (как пиковый, так и мгновенный)
- Сделать иллюстрации исследованных сигналов и поместить их в отчет с описанием
- Оценить возможность передачи звука через телефонный капсюль прямого ТЛФ к полемому телефону
- Поместить в отчет схемы соединений с описанием сигналов и результатов

### ***Практическая работа 2 (4ч.) Запуски регистрация в системе защиты***

Задания:

1. Зарегистрироваться в системе пользователем Администратор, введя пароль «12345».
2. Попытаться загрузить компьютер, затем, три раза подряд неправильно ввести пароль. Какова реакция СЗИ?

### ***Практическая работа 3 (6 ч.) Реализация дискреционной модели разграничения доступа***

Задания:

1. С помощью «Администратора ресурсов» в режиме администрирования разграничить права доступа пользователей к созданным каталогам. Зарегистрироваться пользователем Кравченко. Убедиться, что каталог для этого пользователя не отображается.
2. Зарегистрироваться пользователем Котов и просмотреть содержимое каталога. Убедиться, что каталог для него не отображается.
3. Создать в каталоге пользователем Козлов короткий текстовый файл. Зарегистрироваться Администратором и просмотреть разрешения, которые установлены для вновь созданного файла.
4. Убедиться, что Кравченко сможет прочитать информацию, но не сможет изменить ее.

### ***Практическая работа 4 (6 ч.) Контроль целостности***

Задания:

1. Зарегистрироваться в системе Администратором и настроить контроль целостности всех параметров файла с записью в журнал.
2. Выйти из системы. Зарегистрироваться другим пользователем и внести изменения файлов.
3. Зарегистрироваться Администратором, открыть «Журнал регистрации событий» в программе и найти записи журнала, в которых отражено изменение контрольной суммы файла.

### ***Практическая работа 5 (6 ч.) Гарантированное удаление данных***

Задания:

1. Работая пользователем, создать в каталоге короткий текстовый файл, содержащий произвольную строку символов.

2. Зарегистрироваться другим пользователем. Создать в каталоге текстовый файл, содержащий произвольную строку символов.
3. С использованием редактора WinHEX (или любого другого двоичного редактора), запущенного из основной операционной системы, открыть файл образа диска с установленной СЗИ «Страж NT». Найти и записать смещение, по которому расположены два созданных файла.
4. Удалить файлы, воспользовавшись комбинацией <Shift+Delete> в «Страж NT» (пользователем Администратор).
5. Попытаться найти содержимое удаленных файлов с использованием редактора WinHEX.

***Практическая работа 6 (6 ч.) Реализация мандатной модели разграничения доступа***

Задания:

1. Назначить созданным учетным записям пользователей уровни допуска путем включения их в соответствующие группы.
2. Создать иерархическую структуру каталогов. Назначить созданным каталогам грифы ограничения доступа.

По результатам практических занятий работы обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office 2010 и выше и передаётся преподавателю посредством оговорённой формы связи.

## **АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**

Цель дисциплины: получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от НСД; формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.

Задачи: овладение методами решения профессиональных задач по защите информации от НСД; формирование навыков работы с современными средствами защиты информации от НСД.

В результате освоения дисциплины обучающийся должен:

Знать: процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; организационные меры по защите информации.

Уметь: разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем; выявлять потенциальные уязвимости безопасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем.

Владеть: навыками организации процесса аттестации объектов вычислительной техники и выделенных помещений; навыками сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации сетей; навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы.