**Министерство науки и высшего образования РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Национальный исследовательский университет «МЭИ»**

---

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очно-заочная**

# Рабочая программа дисциплины
# ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

| | |
|---|---|
| **Блок:** | **Блок 1 «Дисциплины (модули)»** |
| **Часть образовательной программы:** | **Вариативная** |
| **№ дисциплины по учебному плану:** | **Б1.В.07.06.01** |
| **Трудоемкость в зачетных единицах:** | **8 семестр - 5;**<br>**9 семестр - 5;**<br>**всего - 10** |
| **Часов (всего) по учебному плану:** | **360 часов** |
| **Лекции** | **8 семестр - 16 часов;**<br>**9 семестр - 16 часов;**<br>**всего - 32 часа** |
| **Практические занятия** | **8 семестр - 16 часов;**<br>**9 семестр - 16 часов;**<br>**всего - 32 часа** |
| **Лабораторные работы** | **8 семестр - 16 часов;**<br>**9 семестр - 16 часов;**<br>**всего - 32 часа** |
| **Консультации** | **9 семестр - 18 часов;** |
| **Самостоятельная работа** | **8 семестр - 131,7 часа;**<br>**9 семестр - 109,5 часов;**<br>**всего - 241,2 часа** |
| **в том числе на КП/КР** | **9 семестр - 16 часов;** |
| **Иная контактная работа** | **9 семестр - 4 часа;** |
| **включая:**<br>**Отчет** | |
| **Промежуточная аттестация:** | |
| **Зачет с оценкой**<br>**Защита курсовой работы**<br>**Экзамен** | **8 семестр - 0,3 часа;**<br>**9 семестр - 0 часов;**<br>**9 семестр - 0,5 часа;**<br>**всего - 0,8 часа** |

**Москва 2017**

**ПРОГРАММУ СОСТАВИЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Рыжиков С.С.<br>Идентификатор: R6eeae99e-RyzhikovSS-b1299f04 | С.С. Рыжиков |
| (должность) | (подпись) | (расшифровка подписи) |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |
| Заведующий выпускающей кафедры | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** освоение общекультурных и профессиональных компетенций, заключающихся в формировании общей готовности студентов к выполнению отдельных мероприятий информационной безопасности применением технических средств защиты информации, а также способности реализовывать техническую защиту информации в интересах обеспечения безопасности хозяйствующего субъекта на основе системного подхода.

**Задачи дисциплины**

- получение студентами знаний и практических навыков в области комплексной защиты объектов информатизации на основе изучения организационных и технических мер защиты информации, технических средств защиты информации, показателей эффективности защиты и методов их оценки, а также основных руководящих, методических и нормативных документов по инженерно-технической защите информации..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Запланированные результаты обучения** |
|---|---|---|
| ОПК-3 способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач | | знать:<br>- назначение, общую характеристику и принципы работы технических средств защиты информации. |
| ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | | знать:<br>- содержание принципов и основ проведения технического контроля защищенности объектов информатизации. |
| ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации | | знать:<br>- перечень, основное содержание и сущность методических и нормативных документов по защите информации.<br><br>уметь:<br>- организовывать проведение и сопровождение аттестации объекта защиты на соответствие требованиям нормативных документов. |
| ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и | | уметь:<br>- контролировать эффективность мер инженерно-технической защиты информации;<br>- определять рациональные меры и технические средства защиты на |

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|---|---|
| эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | | объектах и оценивать их эффективность. |
| ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | | уметь:<br>- разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации. |
| ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов | | знать:<br>- классификацию, общую характеристику и порядок применения технических средств защиты информации, показателей эффективности защиты и методы их оценки. |
| ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации | | уметь:<br>- разрабатывать типовые варианты решений по защите информации. |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 10 зачетных единиц, 360 часов.

| № п/п | Разделы/темы дисциплины/формы промежуточной аттестации | Всего часов на раздел | Семестр | Распределение трудоемкости раздела (в часах) по видам учебной работы | | | | | | | | | | Содержание самостоятельной работы/ методические указания |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Контактная работа | | | | | | | | СР | | |
| | | | | Лек | Лаб | Пр | Консультация | | ИКР | | ПА | Работа в семестре | Подготовка к аттестации /контроль | |
| | | | | | | | КПР | ГК | ИККП | ТК | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | Раздел 1. Способы и технические средства защиты конфиденциальной информации | 84 | 8 | 8 | 8 | 8 | - | - | - | - | - | 60 | - | ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 1. Способы и технические средства защиты конфиденциальной информации" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 1. Способы и технические средства защиты конфиденциальной информации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 1. Способы и технические средства защиты конфиденциальной информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. |
| 1.1 | Введение | 13 | | 1 | 1 | 1 | - | - | - | - | - | 10 | - | |
| 1.2 | Тема 1. Общие положения защиты информации техническими средствами | 13 | | 1 | 1 | 1 | - | - | - | - | - | 10 | - | |
| 1.3 | Тема 2. Способы и технические средства инженерной защиты объектов информатизации | 13 | | 1 | 1 | 1 | - | - | - | - | - | 10 | - | |
| 1.4 | Тема 3. Способы и технические средства обнаружения (поиска) каналов утечки информации | 13 | | 1 | 1 | 1 | - | - | - | - | - | 10 | - | |
| 1.5 | Тема 4. Способы и средства защиты каналов утечки информации | 16 | | 2 | 2 | 2 | - | - | - | - | - | 10 | - | |
| 1.6 | Тема 5. Способы и средства предотвращения | 16 | | 2 | 2 | 2 | - | - | - | - | - | 10 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | утечки информации по материально-вещественному каналу | | | | | | | | | | | | | ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Раздел 1. Способы и технические средства защиты конфиденциальной информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 1. Способы и технические средства защиты конфиденциальной информации" ***Изучение материалов литературных источников:*** [7], 373-396 |
| 2 | Раздел 2. Защита информации техническими средствами в организации | 78 | | 8 | 8 | 8 | - | - | - | - | - | 54 | - | ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 2. Защита информации техническими средствами в организации" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 2. Защита информации техническими средствами в организации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы |
| 2.1 | Тема 6. Характеристика основ организации защиты объектов информатизации в организации | 24 | | 2 | 2 | 2 | - | - | - | - | - | 18 | - | |
| 2.2 | Тема 7. Мероприятия технической защиты объектов информации | 24 | | 2 | 2 | 2 | - | - | - | - | - | 18 | - | |
| 2.3 | Тема 8. Аттестации объекта защиты на | 30 | | 4 | 4 | 4 | - | - | - | - | - | 18 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | соответствие требованиям государственных и корпоративных нормативных документов | | | | | | | | | | | | | ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 2. Защита информации техническими средствами в организации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 2. Защита информации техническими средствами в организации" ***Изучение материалов литературных источников:*** [3], 3-15 [5], 13-60 |
| | Зачет с оценкой | 18.0 | | - | - | - | - | - | - | - | 0.3 | - | 17.7 | |
| | **Всего за семестр** | **180.0** | | **16** | **16** | **16** | - | - | - | - | **0.3** | **114** | **17.7** | |
| | **Итого за семестр** | **180.0** | | **16** | **16** | **16** | - | | - | | **0.3** | **131.7** | | |
| 3 | Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты | 108 | 9 | 16 | 16 | 16 | - | - | - | - | - | 60 | - | ***Подготовка к текущему контролю:*** Повторение материала по разделу "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации" ***Подготовка курсового проекта:*** Курсовой |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | информации | | | | | | | | | | | | | проект выполняется по индивидуальному заданию. В рамках работы необходимо рассчитать основные показатели работы оборудования, выбрать оптимальное решение. Курсовой проект предусматривает пояснительную записку с расчетами и графическую часть. В задание входит расчет следующих показателей:<br>***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации" материалу.<br>***Подготовка к аудиторным занятиям:***<br>Проработка лекции, выполнение и подготовка к защите лаб. работы<br>***Подготовка домашнего задания:***<br>Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.<br>***Подготовка доклада, выступления:***<br>Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в |
| 3.1 | Тема 9. Моделирование защиты информации | 32 | | 4 | 4 | 4 | - | - | - | - | - | 20 | - | |
| 3.2 | Тема 10. Методические рекомендации по разработке мер защиты информации техническими средствами и контроль их эффективности | 38 | | 6 | 6 | 6 | - | - | - | - | - | 20 | - | |
| 3.3 | Тема 11. Проектирование систем инженерно-технической защиты информации | 38 | | 6 | 6 | 6 | - | - | - | - | - | 20 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации" ***Изучение материалов литературных источников:*** [4], 7-28 |
| | Экзамен | 36.0 | | - | - | - | - | 2 | - | - | 0.5 | - | 33.5 | |
| | Курсовая работа (КР) | 36 | | - | - | - | 16 | - | 4 | - | - | 16 | - | |
| | **Всего за семестр** | **180.0** | | **16** | **16** | **16** | **16** | **2** | **4** | **-** | **0.5** | **76** | **33.5** | |
| | **Итого за семестр** | **180.0** | | **16** | **16** | **16** | **18** | | **4** | | **0.5** | **109.5** | | |
| | **ИТОГО** | **360.0** | **-** | **32** | **32** | **32** | **18** | | **4** | | **0.8** | **241.2** | | |

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

**3.2 Краткое содержание разделов**

*1. Раздел 1. Способы и технические средства защиты конфиденциальной информации*

1.1. Введение

Предмет, цели, задачи, содержание и структура дисциплины технические средства защиты информации (ТСЗИ). Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Связь курса с другими дисциплинами. Структура курса Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине..

1.2. Тема 1. Общие положения защиты информации техническими средствами

Задачи и требования к способам и средствам защиты конфиденциальной информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты. Классификация способов и технических средств защиты информации. Физическая защита информации и ее методы. Методы скрытия информации. Понятие информационного портрета и информационных узлов. Методы структурного скрытия. Техническое дезинформирование. Зависимость качества информации от соотношения сигнал/шум. Методы энергетического скрытия сигналов..

1.3. Тема 2. Способы и технические средства инженерной защиты объектов информатизации

Структура системы физической защиты информации. Классификация средств подсистем предупреждения, обнаружения, ликвидации угроз и управления. Естественные и искусственные преграды инженерной защиты. Показатели эффективности инженерной защиты. Способы управления системами физической защиты. Основные средства инженерной защиты информации (заборы, окна, двери, ограждения зданий и помещений, металлические шкафы, сейфы и хранилища) и показатели их защищенности от злоумышленника..

1.4. Тема 3. Способы и технические средства обнаружения (поиска) каналов утечки информации

Способы и средства предотвращения утечки информации с помощью закладных устройств. Классификация технических средств обнаружения (поиска) каналов утечки информации. Технические средства физического поиска каналов утечки информации. Технические средства инструментального (технического) контроля каналов утечки информации. Способы и средства визуального осмотра помещений. Способы и средства обнаружения (поиска) каналов утечки информации за счет ПЭМИН. Классификация средств обнаружения радиоизлучающих и неизлучающих закладных устройств. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Радиоприемные устройства, универсальные поисковые приборы, автоматизированных поисковые комплексы, их состав, возможности, принципы работы, параметры функционирования и порядок применения. Принципы работы нелинейных локаторов. Типы и характеристики отечественных и зарубежных локаторов. Физические принципы работы и способы применения обнаружителей пустот, для выявления закладных устройств..

1.5. Тема 4. Способы и средства защиты каналов утечки информации

Пассивные и активные методы и способы защиты каналов утечки информации. Методы и способы защиты информации обрабатываемой в ТСПИ. Методы и способы защиты информации циркулирующей в телефонных аппаратах и двупроводных линиях. Средства ослабления ПЭМИ ТСПИ и их наводок. Защита электросети, защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонной линии. Защита

информации обрабатываемой техническими средствами. Пассивные способы защиты акустической (речевой) информации от ее утечки через несущие конструкции выделенного помещения. Акустическая защита защищаемого помещения. Активные и комплексные способы защиты акустического информативного сигнала. Способы создания искусственных акустических и виброакустических помех для защиты несущих конструкций и объема защищаемого помещения. Защита пассивными средствами защищаемых помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации. Способы предотвращения несанкционированной записи речевой информации на диктофон. Нейтрализация радиомикрофонов..

1.6. Тема 5. Способы и средства предотвращения утечки информации по материально-вещественному каналу

Способы предотвращения утечки информации по материально-вещественному каналу. Способы очистки демаскирующих веществ. Классификация и характеристика основных технических средств предотвращения утечки информации по материально-вещественному каналу. Технические средства защиты и экстренного уничтожения информации на бумажных носителях. Технические средства защиты и экстренного уничтожения информации на машинных носителях..

## *2. Раздел 2. Защита информации техническими средствами в организации*

2.1. Тема 6. Характеристика основ организации защиты объектов информатизации в организации

Общие требования, предъявляемые к защите информации от технических средств разведки в организации. Классификация видов документов нормативно-правовой базы по защите информации. Руководящие и нормативные документы по организации инженерно-технической защиты, их состав, сущность и основная направленность на уровне государства, ведомства и организации. Состав основных документов нормативно-методической базы, обеспечивающей организацию инженерно-технической защиты информации на предприятии. Краткое содержание положений основных руководящих и нормативных документов государственного и межведомственного уровней. Краткое содержание нормативно-методических документов регламентирующих организацию инженерно-технической защиты информации на предприятии, порядок их разработки и использования..

2.2. Тема 7. Мероприятия технической защиты объектов информации

Основные направления организации защиты объектов информации в организациях. Состав и сущность организационно-технических и технических мер по защите информации в организации. Виды контроля эффективности инженерно-технической защиты информации. Особенности контроля эффективности защиты информации технологических процессов. Меры технического контроля эффективности защиты информации. Характеристика содержания основных организационно-технических мероприятий, определения контролируемых зон и оптимального количества технических средств (ОТСС и ВТСС). Содержание основных технических мероприятий инженерно-технической защиты информации основанных на использовании способов защиты объекта путем скрытия его демаскирующего признака или технической дезинформации путем искажения технических демаскирующих признаков. Содержание и порядок использования мероприятий по контролю эффективности защиты информации..

2.3. Тема 8. Аттестации объекта защиты на соответствие требованиям государственных и корпоративных нормативных документов

Объекты, подлежащие обязательной и добровольной аттестации. Порядок проведения аттестации объектов защиты на соответствие требованиям безопасности информации. Состав и содержание документа «Аттестат соответствия». Категорирование защищаемой информации. Специальные проверки. Порядок проведения специальной проверки технических средств. Специальные обследования. Подготовка к проведению специальных обследований. Оценка вероятного противника, Оценка условий, в которых решается задача выявления технических каналов утечки информации. Порядок и последовательность решения проблемы поисковой операции. Выполнение поисковых мероприятий, радиообнаружение. Первичный осмотр и техническая проверка. Проверка электрических и электронных приборов. Проверка проводных коммуникаций. Подготовка отчетных материалов. Специальные исследования. Общие положения, термины и определения в области специальных исследований. Порядок постановки задачи на выполнение специальных исследований по выявлению и измерению опасных сигналов в каналах возможной утечки информации. Специальные исследования в области защиты речевой информации. Специальные исследования в области акустоэлектрических преобразователей. Специальные исследования в области защиты цифровой информации. Специальные исследования побочных электромагнитных излучений и наводок..

*3. Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации*

3.1. Тема 9. Моделирование защиты информации

Методы организации системы защиты информации на предприятии. Виды моделей системы защиты информации и показатели эффективности. Рекомендации по выбору рациональных вариантов защиты информации и соответствующих средств. Формы представления результатов моделирования..

3.2. Тема 10. Методические рекомендации по разработке мер защиты информации техническими средствами и контроль их эффективности

Типовые рекомендации по выбору мер инженерно-технической защиты информации. Способы оценки значений показателей моделей. Технический контроль эффективности принимаемых мер защиты. Основные средства технического контроля..

3.3. Тема 11. Проектирование систем инженерно-технической защиты информации

Стадии создания системы защиты информации. Предпроектная стадия (предпроектное обследование объекта информатизации, разработка аналитического обоснования создания СЗИ и технического (частного технического) задания на ее создание). Стадия проектирования (разработки проектов) и реализации объекта информатизации. Стадия ввода в действие СЗИ (опытная эксплуатация и приемо-сдаточные испытания средств защиты информации, аттестация объекта информатизации на соответствие требованиям безопасности информации. Содержание документа (проекта, пояснительной записки, предложений) по обеспечению защиты информации в кабинете руководителя. Исходные данные. Постановка задачи. Содержание основной части с обоснованием предложений. Заключение и приложения. Требования к оформлению проекта системы (предложений) при представлении документа на согласование и утверждение..

**3.3. Темы практических занятий**

1. 2.3. Практическая разработка типовых вариантов решений по предотвращению утечки информации за счет побочных электромагнитных излучений и наводок.;
2. 2.2. Формирование основных документов создаваемых при подготовке и проведении аттестации объекта защиты на соответствие его требованиям безопасности информации

и разработке итогового документа «Аттестата соответствия». Методические рекомендации по моделированию угроз и технических каналов утечки информации. Практическая разработка предложений по выбору и размещению технических средств охраны.;
3. 2.1. Порядок разработки и использования методических документов по технической защите информации. Характеристика содержания основных технических мероприятий, определения контролируемых зон и оптимального количества технических средств (ОТСС и ВТСС). Характеристика содержания основных технических мероприятий инженерно-технической защиты информации основанных на использовании технических средств защиты объекта скрытием его демаскирующего признака. Характеристика содержания основных технических мероприятий основанных на использовании способов защиты технической дезинформации и искажения технических демаскирующих признаков. Характеристика основ технического контроля эффективности мер инженерно-технической защиты информации.;
4. 2.4. Практическая разработка предложений по защите информации в кабинете руководителя.;
5. 1.3. Способы и средства защиты информации, обрабатываемой в телефонных аппаратах, циркулирующей в двухпроводных линиях и каналах связи. Назначение, принципы работы и порядок использования технических средств защиты акустической информации в защищаемых помещениях. Назначение, классификация и характеристика основных технических средств используемых для предотвращения утечки информации по материально-вещественному каналу.;
6. 1.2. Назначение, принципы работы и порядок использования технических средств обнаружения радиоизлучающих средств негласного съема информации. Назначение, принципы работы и порядок использования технических средств обнаружения неизлучающих средств негласного съема информации. Назначение, принципы работы и порядок использования технических средств защиты информации обрабатываемой ТСПИ.;
7. 1.1. Классификация методов и технических средств защиты информации. Назначение, состав и характеристика способов и средств инженерной защиты. Назначение, состав и характеристика способов и технических средств обнаружения (поиска) каналов утечки информации. Назначение, принципы работы и порядок использования технических средств визуального поиска закладных устройств и за счет выявления побочного электромагнитного излучения.;
8. 1.4. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области акустоэлектрических преобразований. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области защиты цифровой информации. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области ВЧ-навязывания, ВЧ-облучения и защиты волоконно-оптических линий передачи. Состав и основное содержание требований положений основных руководящих, нормативных и методических документов государственного и межведомственного уровней по организации защиты информации на основе использования технических средств защиты информации. Состав и основное содержание требований положений основных руководящих и методических документов регламентирующих порядок и организацию применения технических средств защиты информации в организации.;
9. 2.5. Порядок проектирования систем технической защиты. Проектный и послепроектный этап проектирования системы защиты информации. Порядок разработки технического задания на создание системы ИТЗИ в организации (Практическое занятие). Порядок разработки технического решения по ТЗИ в

организации и рекомендаций по их вводу в эксплуатацию..

### 3.4. Темы лабораторных работ

1. 2. Лабораторная работа №2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу;
2. 3. Лабораторная работа №3. Методы защиты защищаемого помещения от утечки речевой конфиденциальной информации по акустоэлектрическому каналу.;
3. 4. Лабораторная работа № 4. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля;
4. 5. Лабораторная работа №5. Организация и проведение радиомониторинга объекта защиты автоматизированным комплексом со сканирующим приемником.;
5. 6. Лабораторная работа №6. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ»;
6. 10. Лабораторная работа №10. Специальные исследования в области акустоэлектрических преобразователей.;
7. 8. Лабораторная работа №8 Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.;
8. 9. Лабораторная работа №9 Специальные исследования в области защиты речевой информации.;
9. 1. Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу.;
10. 11. Лабораторная работа №11. Специальные исследования в области защиты цифровой информации.;
11. 12. Лабораторная работа № 12. Специальные исследования побочных электромагнитных излучений и наводок.;
12. 7. Лабораторная работа №7. Специальные проверки по выявлению специальных устройств перехвата (уничтожения) информации в технических средствах..

### 3.5 Консультации

*Аудиторные консультации по курсовому проекту/работе (КПР)*

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации"

*Групповые консультации по разделам дисциплины (ГК)*

1. Обсуждение материалов по кейсам раздела "Раздел 1. Способы и технические средства защиты конфиденциальной информации"
2. Обсуждение материалов по кейсам раздела "Раздел 2. Защита информации техническими средствами в организации"
3. Обсуждение материалов по кейсам раздела "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации"

*Индивидуальные консультации по курсовому проету /работе (ИККП)*

1. Консультации проводятся по разделу "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации"

*Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 1. Способы и технические средства защиты конфиденциальной информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 2. Защита информации техническими средствами в организации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации"

**3.6 Тематика курсовых проектов/курсовых работ**

**9 Семестр**

Курсовая работа (КР)
Темы:
- 1.Разработка технического проекта системы защиты информации в конференц-зале от утечки по параметрическим и оптико-электронному каналам. 2.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустическим и виброакустическим каналам. 3.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустоэлектрическим и оптико-электронному каналам. 4.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по параметрическим и оптико-электронному каналам. 5.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по электромагнитным и акустическим каналам. 6.Разработка технического задания на создание системы защиты информации в кабинете руководителя от утечки по электрическому и параметрическому каналам. 7.Разработка технического задания системы защиты информации в кабинете руководителя от утечки по электромагнитному и акустическому каналам. 8.Разработка технического задания системы защиты информации в кабинете руководителя от утечки по электромагнитному и акустоэлектрическому каналам. 9.Разработка технического задания системы защиты информации в конференц-зале от утечки по электрическим и акустическому каналам. 10.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки речевой информации по акустическим и виброакустическим каналам. 11.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустическим и виброакустическим каналам. 12.Разработка технического проекта системы защиты информации в конференц-зале комнате от утечки по акустическим и виброакустическим каналам. 13.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по акустоэлектрическим и оптико-электронному каналам. 14.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустоэлектрическим и оптико-электронному каналам. 15.Разработка технического проекта системы защиты информации в конференц-зале от утечки по акустоэлектрическим и оптико-электронному каналам. 16.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по параметрическим и оптико-электронному каналам. 17.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по параметрическим и оптико-электронному каналам. 18.Разработка технического проекта системы защиты информации в конференц-зале от утечки по параметрическим и оптико-электронному каналам. 19.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по электромагнитным и электрическим каналам. 20.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по электрическим и параметрическому каналам. 21.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по электромагнитным и акустическим каналам. 22.Разработка технического проекта системы защиты информации в кабинета

руководителя от утечки по электромагнитным и акустоэлектрическому каналам. 23.Разработка технического проекта системы защиты информации в кабинета руководителя от утечки по акустическому и акустоэлектрическому каналам. 24.Разработка программы (технического задания) специального обследования кабинета руководителя по выявлению электронных средств съема информации. 25.Разработка программы (технического задания) специального обследования переговорной комнаты по выявлению электронных средств съема информации. 26.Разработка программы (технического задания) специального обследования конференц-зала по выявлению электронных средств съема информации. 27.Разработка программы (технического задания) специальной проверки по выявлению электронных средств съема информации в технических средствах и системах в кабинете руководителя. 28.Разработка программы (технического задания) специальной проверки по выявлению схемотехнических и иных доработок технических средств и систем в кабинете руководителя, приводящих к усилению их естественных свойств. 29.Разработка программы (технического задания) специального исследования защищенности средств ТСПИ и ВТСС в кабинете руководителя от утечки опасных сигналов ПЭМИН. 30.Разработка программы (технического задания) специального исследования защищенности ограждающих конструкций переговорной комнаты от утечки речевой информации по акустическому и виброакустическому каналам.

**График выполнения курсового проекта**

| Неделя | 1 - 4 | 5 - 8 | 9 - 13 | Зачетная |
|---|---|---|---|---|
| Раздел курсового проекта | 1, 2 | 2, 3 | 3, 4 | Защита курсового проекта |
| Объем раздела, % | 30 | 30 | 40 | - |
| Выполненный объем нарастающим итогом, % | 30 | 60 | 100 | - |

| Номер раздела | Раздел курсового проекта |
|---|---|
| 1 | Введение |
| 2 | Глава первая |
| 3 | Глава вторая |
| 4 | Заключение |

**3.7. Соответствие разделов дисциплины и формируемых в них компетенций**

| Запланированные результаты обучения по дисциплине (в соответствии с разделом 1) | Коды индикаторов | Номер раздела дисциплины (в соответствии с п.3.1) | | | Оценочное средство (тип и наименование) |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | |
| **Знать:** | | | | | |
| назначение, общую характеристику и принципы работы технических средств защиты информации | ОПК-3(Компетенция) | + | | | Отчет/Защита лабораторной работы № 3. Методы защиты защищаемого помещения от утечки речевой конфиденциальной информации по акустоэлектрическому каналу<br>Отчет/Защита лабораторных работ № 1-2. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.каналу |
| содержание принципов и основ проведения технического контроля защищенности объектов информатизации | ПК-1(Компетенция) | | + | | Отчет/Защита лабораторных работ № 4 - 5. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и автоматизированным комплексом со сканирующим приемником<br>Отчет/Защита лабораторных работ № 6.Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ» |
| перечень, основное содержание и сущность методических и нормативных документов по защите информации | ПК-5(Компетенция) | | | + | Отчет/Защита лабораторных работ № 7 - 8. Специальные проверки по выявлению специальных устройств перехвата (уничтожения) информации в технических средствах. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.<br>Отчет/Защита лабораторных работ № 9. Специальные |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | исследования в области защиты речевой информации. |
| классификацию, общую характеристику и порядок применения технических средств защиты информации, показателей эффективности защиты и методы их оценки | ПК-11(Компетенция) | | | + | Отчет/Защита лабораторных работ № 10 - 11. Специальные исследования в области акустоэлектрических преобразователей и в области защиты цифровой информации.<br>Отчет/Защита лабораторных работ № 12. Специальные исследования побочных электромагнитных излучений и наводок. |
| **Уметь:** | | | | | |
| организовывать проведение и сопровождение аттестации объекта защиты на соответствие требованиям нормативных документов | ПК-5(Компетенция) | + | | | Отчет/Защита лабораторной работы № 3. Методы защиты защищаемого помещения от утечки речевой конфиденциальной информации по акустоэлектрическому каналу<br>Отчет/Защита лабораторных работ № 1-2. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.каналу |
| определять рациональные меры и технические средства защиты на объектах и оценивать их эффективность | ПК-6(Компетенция) | | | + | Отчет/Защита лабораторных работ № 10 - 11. Специальные исследования в области акустоэлектрических преобразователей и в области защиты цифровой информации.<br>Отчет/Защита лабораторных работ № 9. Специальные исследования в области защиты речевой информации. |
| контролировать эффективность мер инженерно-технической защиты информации | ПК-6(Компетенция) | | + | | Отчет/Защита лабораторных работ № 4 - 5. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и автоматизированным комплексом со сканирующим приемником<br>Отчет/Защита лабораторных работ № 6.Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | обнаружения радиоизлучающих средств «Крона НМ» |
| разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации | ПК-7(Компетенция) | | | + | Отчет/Защита лабораторных работ № 7 - 8. Специальные проверки по выявлению специальных устройств перехвата (уничтожения) информации в технических средствах. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. |
| разрабатывать типовые варианты решений по защите информации | ПК-12(Компетенция) | | | + | Отчет/Защита лабораторных работ № 12. Специальные исследования побочных электромагнитных излучений и наводок. |

## 4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

### 4.1. Текущий контроль успеваемости

**8 семестр**

Форма реализации: Защита задания

1. Защита лабораторной работы № 3. Методы защиты защищаемого помещения от утечки речевой конфиденциальной информации по акустоэлектрическому каналу (Отчет)
2. Защита лабораторных работ № 1-2. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.каналу (Отчет)
3. Защита лабораторных работ № 4 - 5. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и автоматизированным комплексом со сканирующим приемником (Отчет)
4. Защита лабораторных работ № 6.Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ» (Отчет)

**9 семестр**

Форма реализации: Защита задания

1. Защита лабораторных работ № 10 - 11. Специальные исследования в области акустоэлектрических преобразователей и в области защиты цифровой информации. (Отчет)
2. Защита лабораторных работ № 12. Специальные исследования побочных электромагнитных излучений и наводок. (Отчет)
3. Защита лабораторных работ № 7 - 8. Специальные проверки по выявлению специальных устройств перехвата (уничтожения) информации в технических средствах. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. (Отчет)
4. Защита лабораторных работ № 9. Специальные исследования в области защиты речевой информации. (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

### 4.2 Промежуточная аттестация по дисциплине

*Зачет с оценкой (Семестр №8)*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной составляющих.

*Экзамен (Семестр №9)*

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

*Курсовая работа (КР) (Семестр №9)*

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 9 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1 Печатные и электронные издания:

1. Зайцев, А. П. Технические средства и методы защиты информации : учебник для вузов по группе специальностей "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов . – 7-е изд . – М. : Горячая Линия-Телеком, 2012 . – 442 с. - ISBN 978-5-9912-0233-6 .;
2. Невский, А. Ю. Технические средства охраны : учебное пособие для студентов инженерно-экономического ин-та / А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – М. : ВНИИгеосистем, 2015 . – 186 с. - ISBN 978-5-8481-0196-6 .;
3. Халяпин, Д. Б. Инженерно-техническая защита информации. Лабораторный практикум. Ч.1 : учебное пособие для института безопасности бизнеса МЭИ (ТУ) / Д. Б. Халяпин, А. Ю. Невский ; Ред. Л. М. Кунбутаев ; Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : Издательский дом МЭИ, 2009 . – 88 с. - ISBN 978-5-383-00359-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=402;
4. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : учебное пособие для вузов по специальностям в области информационной безопасности / В. А. Тихонов, В. В. Райх . – М. : Гелиос АРВ, 2006 . – 528 с. - ISBN 5-85438-153-2 .;
5. Северин, В. А. Комплексная защита информации на предприятии : учебник для вузов по направлению и специальности "Юриспруденция" / В. А. Северин ; Ред. Б. И. Пугинский . – М. : Городец, 2008 . – 368 с. - ISBN 978-5-9584020-4-5 .;
6. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
7. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А.- "Технические средства и методы защиты информации", (7-е изд., испр.), Издательство: "Горячая линия-Телеком", Москва, 2018 - (442 с.)
https://e.lanbook.com/book/111057.

### 5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

### 5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/
2. **Научная электронная библиотека** - https://elibrary.ru/
3. **База данных Web of Science** - http://webofscience.com/

4. **База данных Scopus** - http://www.scopus.com
5. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
6. **Портал открытых данных Российской Федерации** - https://data.gov.ru
7. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
8. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
9. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
10. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
11. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
12. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
13. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|---|---|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | К-601, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран |
| | А-300, Учебная аудитория "А" | кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор |
| Учебные аудитории для проведения практических занятий, КР и КП | М-504/1, Учебная аудитория | парта, стол преподавателя, стул, доска маркерная |
| Учебные аудитории для проведения лабораторных занятий | М-504/1, Учебная аудитория | парта, стол преподавателя, стул, доска маркерная |
| Учебные аудитории для проведения промежуточной аттестации | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| | А-300, Учебная аудитория "А" | кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор |
| Помещения для самостоятельной работы | НТБ-303, Компьютерный читальный зал | стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер |
| Помещения для консультирования | А-300, Учебная аудитория "А" | кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, |

| | | |
|---|---|---|
| | | экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор |
| Помещения для хранения оборудования и учебного инвентаря | К-202/2, Склад кафедры БИТ | стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования |

**Приложение А**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Технические средства защиты информации

(название дисциплины)

**8 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Защита лабораторных работ № 1-2. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.каналу (Отчет)

КМ-2 Защита лабораторной работы № 3. Методы защиты защищаемого помещения от утечки речевой конфиденциальной информации по акустоэлектрическому каналу (Отчет)

КМ-3 Защита лабораторных работ № 4 - 5. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и автоматизированным комплексом со сканирующим приемником (Отчет)

КМ-4 Защита лабораторных работ № 6.Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ» (Отчет)

**Вид промежуточной аттестации –** Зачет с оценкой.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
|---|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Раздел 1. Способы и технические средства защиты конфиденциальной информации | | | | | |
| 1.1 | Введение | | + | + | | |
| 1.2 | Тема 1. Общие положения защиты информации техническими средствами | | + | + | | |
| 1.3 | Тема 2. Способы и технические средства инженерной защиты объектов информатизации | | + | + | | |
| 1.4 | Тема 3. Способы и технические средства обнаружения (поиска) каналов утечки информации | | + | + | | |
| 1.5 | Тема 4. Способы и средства защиты каналов утечки информации | | + | + | | |
| 1.6 | Тема 5. Способы и средства предотвращения утечки информации по материально-вещественному каналу | | + | + | | |
| 2 | Раздел 2. Защита информации техническими средствами в организации | | | | | |
| 2.1 | Тема 6. Характеристика основ организации защиты объектов информатизации в организации | | | | + | + |
| 2.2 | Тема 7. Мероприятия технической защиты объектов информации | | | | + | + |
| 2.3 | Тема 8. Аттестации объекта защиты на соответствие требованиям государственных и корпоративных нормативных документов | | | | + | + |
| | | Вес КМ, %: | 25 | 25 | 25 | 25 |

**9 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Защита лабораторных работ № 7 - 8. Специальные проверки по выявлению специальных устройств перехвата (уничтожения) информации в технических средствах. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. (Отчет)

КМ-2 Защита лабораторных работ № 9. Специальные исследования в области защиты речевой информации. (Отчет)

КМ-3 Защита лабораторных работ № 10 - 11. Специальные исследования в области акустоэлектрических преобразователей и в области защиты цифровой информации. (Отчет)

КМ-4 Защита лабораторных работ № 12. Специальные исследования побочных электромагнитных излучений и наводок. (Отчет)

**Вид промежуточной аттестации –** Экзамен.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
|---|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Раздел 3. Проектирование и принципы оценки эффективности системы инженерно-технической защиты информации | | | | | |
| 1.1 | Тема 9. Моделирование защиты информации | | + | + | | |
| 1.2 | Тема 10. Методические рекомендации по разработке мер защиты информации техническими средствами и контроль их эффективности | | | + | + | |
| 1.3 | Тема 11. Проектирование систем инженерно-технической защиты информации | | | | + | + |
| | | Вес КМ, %: | 25 | 25 | 25 | 25 |

**Приложение Б**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Технические средства защиты информации

(название дисциплины)

**9 семестр**

**Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по курсовой работе:**

КМ-1 Соблюдение графика выполнения КР; качество оформления КР
КМ-2 Соблюдение графика выполнения КР; оценка выполнения разделов КР
КМ-3 Соблюдение графика выполнения КР; оценка выполнения разделов КР

**Вид промежуточной аттестации –** защита КР.

| Номер раздела | Раздел курсового проекта/курсовой работы | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 |
|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 13 |
| 1 | Введение | | + | | |
| 2 | Глава первая | | + | + | |
| 3 | Глава вторая | | | + | + |
| 4 | Заключение | | | | + |
| | | Вес КМ, %: | 30 | 30 | 40 |