



Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ
СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

«УТВЕРЖДАЮ»

И.о. проректора

_____ А.В. Троицкий

«__» _____ 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.ДВ.04.03 «ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ
ИНФОРМАЦИИ В ЧАСТИ
ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ РАБОТ (ООО «НОВО», НТЦ
«ЗАРЯ»))»**

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Панцыр Р.Я. Рабочая программа дисциплины (модуля): Государственная система защиты информации в части проведения специальных работ (ООО «НОВО», НТЦ «ЗАРЯ»). – Королев МО: «Технологический Университет», 2023


Рецензент: Воронов А.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н. доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№ 2 от 29.03.2023г.			

**Рабочая программа согласована:
Руководитель ОПОП ВО**

 Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023г.			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является углубленное изучение теоретических и прикладных основ социальной инженерии как научной дисциплины, связанной с созданием средств и методов выработки научно обоснованных управленческих решений в области информационной безопасности

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

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

Профессиональные компетенции:

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.

Основными задачами дисциплины являются:

- раскрытие сущности, целей социальной инженерии (СИ) как метода несанкционированного доступа к информации или системам хранения информации без использования технических средств;

- определение общих методологических подходов построения систем защиты информации с учетом возможных атак с использованием технологии социальной инженерии;

- освоение методических подходов, установления состава защищаемой информации и выявления объектов защиты, подверженных атакам со стороны социального хакерства;

- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников, использующих методы социальной инженерии);

- овладение методами оценки уязвимости защищаемой информации;

- определение методов выявления параметров и структуры систем защиты информации;

- освоение методов установления целесообразного состава мероприятий по защите информации от социального хакерства;

- определение методологических подходов оценки эффективности мер по защите информации от воздействия со стороны атак с использованием методов социальной инженерии.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-5.3. Применяет методы и навыки эффективного межкультурного взаимодействия, обеспечивает создание дружественной, деловой среды взаимодействия при выполнении профессиональных задач;

- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.

Необходимые умения:

- УК-5.2. Анализирует и учитывает разнообразие культур в процессе межкультурного взаимодействия, выстраивает профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп

- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.

Необходимые знания:

- УК-5.1. Использует технологии эффективного межкультурного взаимодействия, анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, обосновывает актуальность их использования при профессиональном взаимодействии

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Государственная система защиты информации в части проведения специальных работ» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина «Государственная система защиты информации в части проведения специальных работ» базируется на ранее изученных дисциплинах: «Современная философия и методология науки»; «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: УК-1, 2; ПК-1, 3; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базой для обеспечения информационной безопасности», прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа

Виды занятий	Всего часов	Семестр 2
Общая трудоемкость	72	72
Аудиторные занятия	38	38
Лекции (Л)	16	16
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)		
Другие виды контактной работы*	6	6
Практическая подготовка	нет	нет
Самостоятельная работа	34	34
Курсовые, расчетно-графические работы		
Контроль самостоятельной работы студентов	+	+
Контрольная работа, домашнее задание	+	+
Текущий контроль знаний (7 - 8, 15 - 16 недели)		ТестТтТтт
Вид итогового контроля	Зачет	Зачет

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очно	Практически занятия, час. Очно	Занятия в интерактивной форме, час. Очно	Код компетенций
Раздел I. Обеспечение безопасного допуска к информационным ресурсам				
Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература	1	1	1	ПК-1 ПК-2
Тема 2. Функции, состав, структура и задачи государственной системы защиты информации	1	1		ПК-1 ПК-2,
Тема 3. Нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации	1	1	1	УК-5 ПК-2
Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ (СЗИ)	1	1		УК-5 ПК-2

и проведение аттестации объектов информатизации				
Тема 5. Основные положения законодательства в области защиты информации	1	1	-	УК-5 ПК-1
Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе	1	1		УК-5 ПК-1
Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации	1	1		УК-5 ПК-1 ПК-2
Тема 8. Проведение аттестация объектов информатизации (ОИ)	1	1	1	УК-5 ПК-1 ПК-2
Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации	1	1	1	УК-5 ПК-1 ПК-2
Тема 10. Этапы практического проведения работ по аттестации объектов информатизации	1	1		УК-5 ПК-1 ПК-2
Тема 11. Проверка и испытание аттестуемого объекта информатизации	1	1		УК-5 ПК-1 ПК-2

Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам	1	1	1	УК-5 ПК-1 ПК-2
Тема 13. Пассивные и активные методы защиты объектов информатизации	1	1	-	УК-5 ПК-1 ПК-2
Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	1	1	-	УК-5 ПК-1 ПК-26
Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа	1	1		УК-5 ПК-1 ПК-26
Тема 16. Методики оценки защищённости объектов информатизации	1	1	1	УК-5 ПК-1 ПК-2
Итого:	16	16	6	

4.2. Содержание тем дисциплины

Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий.

Рекомендуемая литература

Значение, предмет изучения и краткое содержание курса «Аттестация объектов информации». Место дисциплины среди других курсов, изучаемых студентами. Методы изучения дисциплины. Названия тем, распределение их по видам аудиторных занятий. Форма проверки знаний. Научная, учебная и периодическая литература по дисциплине. Знания, умения и

компетенции, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных понятий по аттестации объектов информации применительно к изучению курса. Нормативно-методические документы, регулирующие вопросы аттестации объектов информатизации.

Тема 2. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).

Что такое ГСЗИ, ее функции, состав, структура и задачи.

Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

Функции федерального органа по сертификации и аттестации.

Функции органов по аттестации.

Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации

Содержание Положения о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27.10.1995 № 199.

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

Содержание Положения об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание Типового положения об испытательной лаборатории, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание руководящих документов Гостехкомиссии России в области аттестации объектов информатизации. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К). Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.

Основное содержание Требований к системам обнаружения вторжений, утверждённых приказом ФСТЭК России от 06.12.2011 № 638.

Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей

сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утверждённого приказом ФСТЭК России от 15.03.2012 № 27. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).

Содержание Порядка проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Содержание национальных стандартов в области аттестации объектов информатизации.

Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ и проведение аттестации объектов информатизации

Содержание Федерального закона от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности».

Содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации". Содержание Приказ ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"

Содержание Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

Тема 5. Основные положения законодательства в области защиты информации

Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности». Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Основное содержание Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.

Выполняемые работы на предпроектной стадии по обследованию объекта информатизации; содержание аналитического обоснования необходимости создания системы защиты информации; содержание технического задания на разработку системы защиты информации; содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)

Основные требования и рекомендации по защите речевой КИ.

Защита КИ, циркулирующей в системах звукоусиления и звукового сопровождения.

Основное содержание и требования СНиП 23-03-2003. Защита от шума.

Тема 8. Проведение аттестации объектов информатизации (ОИ)

Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.

Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации

Перечень работ по подготовке объекта информатизации к аттестации.

Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.

Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

Тема 10. Этапы практического проведения работ по аттестации объектов информатизации

Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.

Последовательность проведения работ по аттестации защищаемых помещений.

Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.

Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

Тема 11. Проверка и испытание аттестуемого объекта информатизации

Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам

Содержание работ по поставке средств защиты информации от утечки по техническим каналам.

Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

Тема 13. Пассивные и активные методы защиты объектов информатизации

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.

Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке

Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа

Общие требования и рекомендации по защите информации (ЗИ) в автоматизированных системах (АС). Основные требования и рекомендации по ЗИ.

Методика формирования комплекса мероприятий по защите информационных систем в условиях возможного воздействия злоумышленников.

Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.

Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

Тема 16. Методики оценки защищённости объектов информатизации

Методика оценки защищённости помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

Методика оценки защищённости ОТСС от утечки конфиденциальной информации (КИ) за счёт наводок на токоведущие коммуникации.

Временная методика оценки защищённости помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Государственная система защиты информации в части проведения специальных работ (ООО «НОВО», НТЦ «ЗАРЯ»))» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью». Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5178> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 5 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 166 с. — ISBN 978-5-9912-0275-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5182> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 4 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 214 с. — ISBN 978-5-9912-0274-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5181> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

4. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5179> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал;
2. <http://informika.ru/> – образовательный портал;
3. www.wikIsec.ru - Энциклопедия информационной безопасности. –

Публикации, статьи;

4. www.biblioclub.ru - Универсальная библиотека онлайн;
5. www.rucont.ru - ЭБС «Рукопт»;
6. <http://www.academy.it.ru/> – академия АИТИ;
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов

Российской Федерации;

8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации;

9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;

10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю;

11. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации;

12. <http://www.gov.ru> - Официальный сервер органов государственной власти Российской Федерации;

13. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;

14. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice.
- **Информационные справочные системы:**
 1. Электронные ресурсы информационно-образовательной среды Университета.
 2. Информационно-справочные системы (Консультант+; Гарант).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
 - рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
 - рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задание

ЗАДАНИЕ № 1

Тема: Средства защиты информации

Цель работы.

Изучение теоретической основы активных средств защиты. Изучение основных аспектов настройки и эксплуатации средств защиты.

Продолжительность занятия: полтора учебных часа.

Задания.

1. Изучить теоретическую часть Задания №1.
2. Выполнить практическую часть Задания №1:
 - а) ответить на вопросы для самопроверки;
 - б) выполнить практические задания.
3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Целью защиты информации от утечки по ТКУИ является уменьшение отношения «сигнал/шум». Уменьшение может осуществляться с помощью применения пассивных и/или активных методов и средств защиты.

Активный метод заключается в перекрытии полезного сигнала более мощным шумом. Данный метод защиты осуществляется аппаратное, через специальные устройства так называемые «Генератор шума». Генераторы шумов специально создают мощные электромагнитные излучения, которые не имеют информативной ценности и затрудняют или делают совсем невозможным анализ полезного сигнала относительно окружающего шума. Надо заметить, что генераторы шумов от побочных электромагнитных излучений имеют свои недостатки, такие как:

- довольно мощные источники излучения не являются полезным для здоровья;
- наличие маскирующего сигнала говорит о наличие конфиденциальной информации;
- нельзя гарантировать абсолютную защищенность информации.

Пассивный метод заключается в уменьшении мощности самого излучаемого сигнала. Осуществление подобного метода заключается в изоляции излучающих проводников, устройств, а также периметра помещения специальными материалами поглощающими ЭМП, в отношении проводных линий – установка фильтров.

Активные методы основаны на увеличении уровня шума путем применения генераторов пространственного зашумления. Данные устройства, как правило, формируют широкополосную помеху во всем диапазоне частот. Регулировка в большинстве моделей осуществляется только по общему уровню сигнала, за редким исключением присутствует возможность корректировки частотной характеристики на низких, средних и высоких частотах.

С точки зрения заключения договора на аттестацию ОИ применение САЗ самый удобный и простой вариант, а иногда и единственный (если организация арендует 1-2 помещения и расстояние до границы КЗ 1 м).

Наиболее популярные модели САЗ по каналу ПЭМИН приведены. приведен скан сертификата ФСТЭК России на САЗ «Соната-РЗ.1».

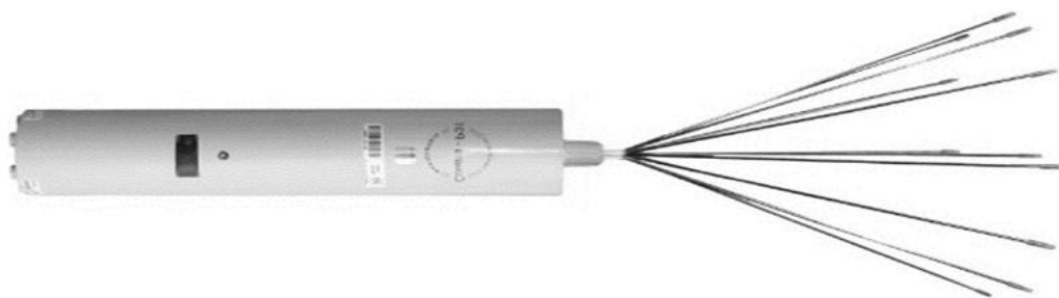


Рисунок 1. Средство активной защиты от утечек за счет ПЭМИН
«Соната-РЗ.1»

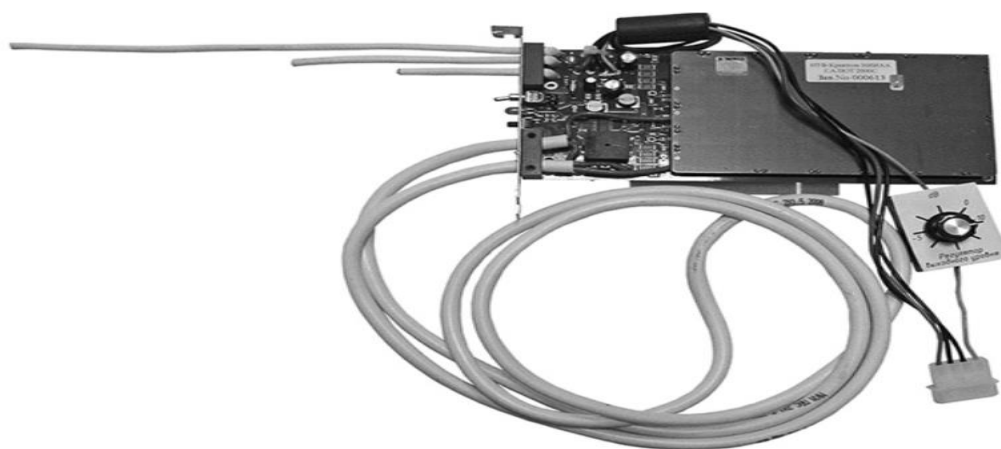


Рисунок 2. Средство активной защиты информации от утечек за счет
ПЭМИН «Салют 2000С»

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 3539

Выдан 24 марта 2016 г.
Действителен до 24 марта 2019 г.

Настоящий сертификат удостоверяет, что средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Соната-Р3.1», разработанное и производимое ООО «Анна» в соответствии с техническими условиями ЮДИН.665820.015 ТУ, является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа «А» и «Б», соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по 2 классу защиты, может применяться в выделенных помещениях до 1 категории включительно.

Рисунок 3. Сертификат соответствия ФСТЭК России на СЗИ «Соната-Р3.1»

Исходя из графика спектров помех можно сделать вывод, что во всем диапазоне частот помехи не обладают равномерным спектром. Вследствие чего, при проведении измерений, сигналы ПЭМИ могут оказаться на частотах, соответствующих «провалам» в спектре помехи, что поставит под вопрос защищенность объекта. Проблема в том, что с точки зрения требований по сертификации САЗ по каналу ПЭМИН, оценивается только спектральная плотность мощности, причем в достаточно широкой полосе, а то, как ведет себя спектр помехи в данной полосе это уже будет видно на практике (для примера приведем характеристики САЗ «Соната-Р2», табл. 2–4).

Т а б л и ц а 2

Спектральная плотность напряженности электрической составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Вертикальная поляризация, дБ		Горизонтальная поляризация, дБ	
	Без дополни- тельной антенны	С дополни- тельной антенной	Без дополни- тельной антенны	С дополни- тельной антенной
от 0,01 до 0,15	50	80	50	80
от 0,15 до 1	45	70	40	70
от 1 до 5	45	60	40	55
от 5 до 30	45	60	40	50
от 30 до 100	40	50	40	50
от 100 до 1000	30	30	30	30
от 1000 до 2000	30	30	30	30

Таблица 3

**Спектральная плотность напряженности магнитной составляющей ЭМП
«Соната-Р2», не менее**

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,15	30	30
от 0,15 до 4	35	35
от 4 до 10	40	40
от 10 до 30	30	35

Таблица 4

**Спектральная плотность напряжения помех в линиях электропитания
и заземления «Соната-Р2», не менее**

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,04	25	25
от 0,04 до 10	35	35
от 10 до 100	35	45
от 100 до 600	25	25
от 600 до 1000	15	15

Пассивные методы защиты информации от утечки по каналам ПЭМИН возможно реализовать следующими путями:

- уменьшение уровня информативного сигнала за счет экранирования помещения (что практически невозможно, гарантию может дать только специализированная экран камера, которая применяется для лабораторных исследований источников радиосигналов).

- если в процессе анализа выявлено, что ТКУИ возникает только за счет наводок на линии электропитания, то возможно применение сетевых подавляющих фильтров (рисунок 3).



Рисунок 3. Фильтр сетевой помехоподавляющий ЛФС-10-1Ф

Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц

«ЛФС-10-1Ф» соответствует: типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.

«ЛФС-10-1Ф» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.

Отметим, что на практике чаще всего в случае невыполнения норм защищенности применяются средства активной защиты – генераторы электромагнитного шума, которые также создают наведенную помеху на линии и токоведущие коммуникации.

Практическая часть.

Вопросы для самопроверки:

- 1) Опишите самый простой и удобный способ на аттестацию ОИ при применении САЗ.
- 2) По какому классу защиты соответствует ЛФС-10-1Ф?
- 3) Что такое активная защита САЗ?
- 4) Что такое пассивная защита САЗ?
- 5) Какими методами по защите информации от утечек ПЭМИН возможно реализовать пассивные меры защиты?

Практические задания:

По вашему мнению, является ли допустимым использование одновременно и пассивных и активных мер защиты? Если возможно, в подробности расскажите почему?

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ (МОДУЛЮ)**

**ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В
ЧАСТИ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ РАБОТ
(ООО «НОВО», НТЦ «ЗАРЯ»)**

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Тема:1,3,4,9,11	УК-5.3. Применяет методы и навыки эффективного межкультурного взаимодействия, обеспечивает создание дружественной, деловой среды взаимодействия при выполнении профессиональных задач;	УК-5.2. Анализирует и учитывает разнообразие культур в процессе межкультурного взаимодействия, выстраивает профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп	УК-5.1. Использует технологии эффективного межкультурного взаимодействия, анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, обосновывает актуальность их использования при профессиональном взаимодействии
2.	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.	Тема:2,4,5,12,13 Тема:1,4,7,10,11,15, 16	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированных	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

				анной ИАС.		
3.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Тема:1,4,7,8,12	ПК-1.3. Управлять работой коллектива профессионалов в ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.	ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность	ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатации защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

Код компетенции	Инструменты, оценивающие сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
УК-5 ПК-1 ПК-2	Доклад	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
УК-5 ПК-1,2	<i>Тест</i>	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов; • компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов; <p>В) не сформирована (компетенция <u>не</u></p>	<p>Например:</p> <p>Проводится письменно. Время, отведенное на процедуру - 30 минут.</p> <p>Неявка – 0 баллов.</p> <p>Критерии оценки определяются процентным соотношением.</p> <p>Неудовлетворительно – менее 50% правильных ответов.</p> <p>Удовлетворительно - от 51% правильных ответов.</p> <p>Хорошо - от 70%.</p> <p>Отлично – от 90%.</p> <p>Максимальная оценка – 5 баллов.</p>

		<i>сформирована) – менее 50% правильных ответов</i>	
УК-5; ПК-1,2	Контрольная работа	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> • <i>компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> • <i>компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p>	<p>1. Проводится устно в форме защиты отчета</p> <p>2. Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1. Соответствие оформления требованиям (1 балл).</p> <p>2. Соответствие разработанного устройства техническому заданию (1 балл)</p> <p>3. Моделирование работы разработанного устройства (1 балл)</p> <p>4. Качество и количество используемых источников (1 балл)</p> <p>5. Правильность и полнота ответов на контрольные вопросы (1 балл)</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.</p>

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.

9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

Примерная тематика заданий на контрольную работу:

1. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
5. Компьютерная преступность в экономических областях.
6. Мир XXI века: информационное противоборство.
7. Компьютерные вирусы в современных информационных системах.
8. Информационные угрозы современным экономическим объектам.
9. Информатизация России и проблема защиты информации.
10. Безопасность информации в коммерческой деятельности.
11. Разведки России – исторический аспект.
12. Мировой информационный терроризм.
13. Этика защиты информации.
14. Становление и развитие промышленного шпионажа.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Государственная система защиты информации в части проведения специальных работ (ООО «НОВО», НТЦ «ЗАРЯ»)» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	УК-5; ПК-1,2	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%</i>
Согласно учебному плану	тестирование	УК-5; ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от</i>

						90%
Согласно учебному плану	Зачет	УК-5; ПК-1,2	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: «Зачтено»: 1. знание лексического и грамматического материала; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях в течение семестра; 4. ответ на вопросы зачета. «Не зачтено»: 1. демонстрирует частичные знания по темам дисциплин; 2. незнание лексического и грамматического материала; 3. неумение использовать и применять полученные знания; 4. не работал на практических занятиях; 5. не отвечает на вопросы зачета.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

Тестовые задания для контроля остаточных знаний

1. Что понимается под аттестацией объектов информатизации?
 - контрольная проверка объекта информатизации, по результатам которой выдается сертификат соответствия требованиям по безопасности информации;
 - оснащение объекта информатизации средствами защиты, по результатам которой выписывается паспорт или паспорт соответствия требованиям по безопасности информации;
 - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - аттестата

соответствия подтверждается, что объект соответствует требованиям стандартов;

- комплекс организационно-технических мероприятий, в результате которых посредством специального документа - лицензии подтверждается, что объект соответствует требованиям стандартов.

2. Какие объекты информатизации подлежат обязательной аттестации?

- объекты информатизации, предназначенные для обработки конфиденциальной информации в коммерческих организациях;
- объекты информатизации, предназначенные для обработки конфиденциальной информации в бюро кредитных историй;
- объекты информатизации, предназначенные для обработки информации, составляющие государственную тайну, управления экологически опасными объектами, ведения секретных переговоров ;
- объекты информатизации, предназначенные для обработки информации, составляющей коммерческую тайну.

3. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?

- технический паспорт объекта информатизации;
- матрицу доступа к объекту вычислительной техники, аттестованному по требованиям безопасности информации;
- протоколы испытаний и заключение по результатам проведения специальных исследований объекта информатизации;
- аттестат соответствия объекта информатизации требованиям по безопасности информации.

4. Какие классы защищенности от несанкционированного доступа реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации?

- 1А, 1Б, 1В;
- 2А, 3А;
- 2Б, 3Б;
- 1Г, 1Д.

5. Когда проводят испытания несертифицированной продукции, используемой на объекте информатизации, подлежащем обязательной аттестации?

- в ходе проведения аттестационных испытаний объекта информатизации;
- после предварительного ознакомления с объектом аттестации;
- после оформления, регистрации и выдачи аттестата соответствия;
- до подачи и рассмотрения заявки на аттестацию объекта информатизации.

1.2. Типовые вопросы, выносимые на зачет

1. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).
2. Основные нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации.
3. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации защищаемых помещений по требованиям безопасности информации.
4. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
5. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
6. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.
7. Последовательность проведения работ по аттестации защищаемых помещений.
8. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации объектов вычислительной техники по требованиям безопасности информации.
9. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.
10. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?
11. Перечислить и пояснить классы защищенности от несанкционированного доступа, которые реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации.
12. Порядок проведения аттестации объекта информатизации.
13. Перечень и содержание документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.
14. Перечень и содержание документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.
15. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.
16. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.
17. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

18. Документы, оформляемые и разрабатываемые при проверках и испытаниях аттестуемого объекта информатизации в процессе его эксплуатации.

19. Основные положения методики оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации; оценка защищённости помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

20. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации.

21. Основные положения методики оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.

22. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

23. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).

24. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.

25. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.

26. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К).

27. Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.

28. Основное содержание Требований к системам обнаружения вторжений, утвержденных приказом ФСТЭК России от 06.12.2011 № 638.

29. Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утвержденного приказом ФСТЭК России от 15.03.2012 № 27.

30. Основное содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).

31. Основное содержание Порядка проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

32. Основное содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

33. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

34. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации".

35. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"

36. Основное содержание ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

37. Основное содержание ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования

**Методические указания для обучающихся по освоению дисциплины
(модуля)**

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В
ЧАСТИ ПРОВЕДЕНИЯ СПЕЦИАЛЬНЫХ РАБОТ
(ООО «НОВО», НТЦ «ЗАРЯ»)**

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Целью изучения дисциплины является формирование у студентов базовых знаний и практических навыков в области проведения аттестации объектов информатизации по требованиям безопасности информации.

Задачи дисциплины:

- формирование у студентов базовых знаний в области аттестации объектов информатизации по требованиям безопасности информации, проведению специального обследования (СО), специальных проверок (СП) и специальных исследований, проводимых в ходе аттестации;
- ознакомление с основными нормативно-правовыми и методическими документами в области проведения специальных исследований и аттестации объектов информатизации по требованиям безопасности информации;
- привитие навыков практической работы с контрольно-измерительной аппаратурой, применяемой для аттестации объектов информатизации;
- привитие навыков разработки организационно-распорядительных документов, оформляемых по результатам аттестации объектов информатизации.

2. Указания по проведению практических занятий

Тема 1- 2. Введение. Функции, состав, структура и задачи государственной системы защиты информации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 1.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Функции государственной системы защиты информации в соответствии с основными правовыми и нормативно методическими документами.

2. Состав, структура и задачи государственной системы защиты информации в соответствии с основными правовыми и нормативно методическими документами.

Продолжительность занятия: 1 ч.

Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 2.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических методов защиты информации.

Основные положения темы занятия:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Положение о сертификации средств защиты информации по требованиям безопасности информации.
2. Руководящие документы Гостехкомиссии России, используемые при аттестации объектов информатизации, и их содержание.
3. Основное содержание национальных стандартов в области аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств защиты информации (СЗИ) и проведение аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 3.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

Основные положения темы занятия:

- базовые протоколы криптографической защиты информации.
- квантовая криптография.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).
2. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.
3. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 5. Основные положения законодательства в области защиты информации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 4.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки управления ключами.

Основные положения темы занятия:

- Управление ключами.
- Взаимодействие с УЦ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Конституция РФ, федеральные законы, Указы Президента РФ, постановления и распоряжения Правительства РФ об информационной безопасности общества и его граждан.

2. Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности».

3. Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. Основное содержание Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

6. Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Продолжительность занятия: 1 ч.

Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 5.

Учебные вопросы

1. Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.
2. Выполняемые работы на предпроектной стадии по обследованию объекта информатизации;
3. Содержание аналитического обоснования необходимости создания системы защиты информации;
4. Содержание технического задания на разработку системы защиты информации;
5. Содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

Продолжительность занятия: 1 ч.

Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *беседа..*

Практическое занятие 6.

Учебные вопросы

1. Основные требования и рекомендации по защите речевой КИ.
2. Защита КИ, циркулирующей в системах звукоусиления и звукового сопровождения.

Продолжительность занятия: 1 ч.

Тема 8. Проведение аттестации объектов информатизации (ОИ)

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 7.

Учебные вопросы

1. Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.

2. Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

Продолжительность занятия: 1 ч.

Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: практическая работа в группах.

Практическое занятие 8.

Учебные вопросы

1. Перечень работ по подготовке объекта информатизации к аттестации.

2. Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.

3. Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

3. Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

Продолжительность занятия: 1 ч.

Тема 10. Этапы практического проведения работ по аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 9.

Учебные вопросы

1. Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.

2. Последовательность проведения работ по аттестации защищаемых помещений.

3. Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.

4. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

Продолжительность занятия: 1 ч.

Тема 11. Проверка и испытание аттестуемого (аттестованного) объекта информатизации

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *беседа.*

Практическое занятие 10.

Учебные вопросы

1. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.
2. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.
3. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

Продолжительность занятия: 1 ч.

Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам

Вид практического занятия: занятие в смешанной форме
Образовательные технологии: *групповая дискуссия.*

Практическое занятие 11.

Учебные вопросы

1. Содержание работ по поставке средств защиты информации от утечки по техническим каналам.
2. Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 13. Пассивные и активные методы защиты объектов информатизации

Вид практического занятия: занятие в смешанной форме
Образовательные технологии: *групповая дискуссия.*

Практическое занятие 12.

Учебные вопросы

1. Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.
2. Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

Продолжительность занятия: 1 ч.

Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке

Вид практического занятия: занятие в смешанной форме
Образовательные технологии: *беседа.*

Практическое занятие 13.

Учебные вопросы

1. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
2. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
3. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Продолжительность занятия: 1 ч.

Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 14.

Учебные вопросы

1. Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.
2. Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

Продолжительность занятия: 1 ч.

Тема 16. Методики оценки защищённости объектов информатизации

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 15.

Учебные вопросы

1. Методика оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание; оценка защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.
2. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации.
3. Методика оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.
4. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

Продолжительность занятия: 2 ч.

3. Указания по проведению лабораторных работ

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Введение. Основные понятия теории компьютерной безопасности	<p>Подготовка докладов и презентаций по темам:</p> <p>Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.</p> <p>Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.</p> <p>Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>
2.	Анализ угроз информационной безопасности для компьютерных систем	<p>Подготовка докладов и презентаций по темам:</p> <p>Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.</p> <p>Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.</p> <p>Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и</p>

		<p>способы вторжения в устойчивую работу автоматизированных систем злоумышленников.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>
3	<p>Основные уровни защиты информации компьютерных системах</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.</p> <p>Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.</p> <p>Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>
4	<p>Основные положения формальной теории защиты информации</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Перечень основных документов ФСТЭК России по вопросам защиты информации.</p> <p>Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>
5	<p>Формальные модели безопасности</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ.</p> <p>Базовая модель угроз ИСПДн.</p> <p>Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>

6	<p>Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Лицензирование и сертификация в области защиты информации.</p> <p>Комплексные системы защиты информации.</p> <p>Аттестация АС по требованиям безопасности информации.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>
7	<p>Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).</p> <p>Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.</p> <p>Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.</p> <p><i>Подготовка рефератов, письменная работа, самостоятельное изучение тем.</i></p>

**Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:**

1. Место информационной безопасности в системе национальной безопасности.
2. Современная концепция информационной безопасности.
3. Цели и концептуальные основы защиты информации.
4. Критерии, условия и принципы отнесения информации к защищаемой.
5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
6. Понятие и структура угроз защищаемой информации.

7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
8. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
9. Виды уязвимости информации и формы ее проявления.
10. Каналы и методы несанкционированного доступа к конфиденциальной информации.
11. Модель нарушителя.
12. Модель угроз.
13. Критерии оценки безопасности информационных технологий.
14. Методы защиты информации от несанкционированного доступа.
15. Риски информационной безопасности.

Примерные темы докладов

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью». Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5178> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 5 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 166 с. — ISBN 978-5-9912-0275-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5182> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 4 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 214 с. — ISBN 978-5-9912-0274-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5181> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

4. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью». Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5179> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. <http://www.academy.it.ru/> - академия АЙТИ.
7. <http://www.minfin.ru/> - **Официальный сайт Министерства финансов Российской Федерации**
8. <http://www.gov.ru/> - **Официальный сервер органов государственной власти Российской Федерации.**
9. <http://www.fsb.ru/> - **Официальный сайт Федеральной Службы Безопасности**
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю
11. <http://www.minfin.ru> - **официальный сайт Министерства финансов Российской Федерации.**
12. <http://www.gov.ru> - **сервер органов государственной власти Российской Федерации.**

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).