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

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.03 «КОМПЛЕКСНЫЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (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: Комплексный аудит информационной безопасности автоматизированных автоматизированных систем (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	№8 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.			

2

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является:

овладение основными правилами, принципами, закономерностями, методами моделирования информационных процессов и технологий для обеспечения информационной безопасности;

умение эффективно использовать методы моделирования на практике.

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

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.
- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.

Основными задачами дисциплины являются:

- подготовить магистров к самостоятельному научному творчеству в области защищенности информационных систем;
- расширить представление в области организации научных исследований по моделированию информационных процессов и технологий;
- систематизировать знания в плане организации научных исследований и достижения результатов в процессе моделирования информационных систем и технологий;
- овладеть навыками решения творческих нетривиальных задач связанных с вопросами моделирования угроз информационным объектам и противодействия им.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- 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.
- 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.

Необходимые умения:

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

Необходимые знания:

- 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 (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина 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 базируется на ранее изученных дисциплинах «Основы теории информационной безопасности», «Специальные разделы математики», «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» и компетенциях: ПК-1, 3; УК-1, 2; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин общенаучного цикла «Компьютерное моделирование информационных процессов и технологий», «Комплексная проверка информационной безопасности» и для написания магистерской диссертации..

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины представлена в таблице 1 и составляет 2 зачетные единицы, 72 часа.

Таблица1

Виды занятий	**Всего часов**	**Семестр 3**	**Семестр …**	**Семестр …**	**Семестр …**
Общая трудоемкость	**72**	**72**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**46**	**46**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	8	8			
Практическая подготовка	**4**	**4**			
Другие виды контактной работы*	**6**	**6**			
Самостоятельная работа	**26**	**26**			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	-	-			
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	Практические занятия, час. Очно	Лабораторные работы час. Очно	Занятия в интерактивной форме, час. Очно	**Практическая поготовка ,час**	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	0.25	0.25		ПК-1
Тема 2. Функции, состав, структура и задачи государственной системы защиты информации	1	1	0.25	0.25		ПК-1
Тема 3. Нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации	1	1	0.25	0.25		ПК-1
Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ (СЗИ) и проведение аттестации объектов информатизации	1	1	0.25	0.25		ПК-2
Тема 5. Основные положения законодательства в области защиты информации	1	1	0.25	1		ПК-2
Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе	1	1	0.25	1		ПК-2
Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации	1	1	0.25	1		ПК-2
Тема 8. Проведение аттестация объектов информатизации (ОИ)	1	1	0.25	1		ПК-1,2
Тема 9. Перечень документов и работ по подготовке объекта информатизации к	1	1	0.25	1		ПК-1,2

аттестации						
Тема 10. Этапы практического проведения работ по аттестации объектов информатизации	1	1	0.25	1		ПК-1,2
Тема 11. Проверка и испытание аттестуемого объекта информатизации	1	1	0.25	1		ПК-1,2
Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам	1	1	0.25	1		ПК-1,2
Тема 13. Пассивные и активные методы защиты объектов информатизации	1	1	0.25	0.25	1	ПК-1,2
Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	1	1	0.25	0.25	1	ПК-1,2
Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа	1	1	0.25	0.25	1	ПК-1,2
Тема 16. Методики оценки защищённости объектов информатизации	1	1	0.25	0.25	1	ПК-1,2
Итого:	16	16	4	10	4	

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 и 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 с системах звукоусиления и звукового сопровождения.

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

Тема 8. Проведение аттестация 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 защиты 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 защищенности 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 защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Комплексный аудит информационной безопасности» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы.

Основная литература:

1.Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
4.Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (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 «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 **- 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 (модуля)

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 (модуля)

- **Перечень программного обеспечения:** MSOffice.
- **Информационные справочные системы:**

1.Электронные ресурсы 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.

Практические занятия целесообразно проводить в специализированной учебной лаборатории кафедры информационной безопасности с использованием имеющихся технических средств:

1. Имитатор многофункциональный ИМФ-2;
2. Многофункциональный комплекс радиоконтроля «Омега»;
3. Измеритель шума и вибраций ВШВ-003-М3;
4. Поисковый приемник радиосигналов «Скорпион».
5. Селективные микровольтметры;
6. Анализатор спектра;

Лабораторные работы:

- компьютерная аудитория, оснащенная программно-аппаратными средствами защиты информации и аудита компьютерной безопасности, а также оснащенная специализированным оборудованием и контрольно-измерительной аппаратурой.

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.

Приложение 1

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)

КОМПЛЕКСНЫЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

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 компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Тема:1 - 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 автоматизированной ИАС.	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.
2	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном	Тема 1-16	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем,

		исполнении.		оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	***Инструменты, оценивающие сформированность компетенции***	***Показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
ПК-1,2	***Тест***	***А) полностью сформирована (компетенция освоена на высоком уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 70% правильных ответов;*** • ***компетенция освоена на базовом уровне – от 51% правильных ответов;*** ***В) не сформирована (компетенция не сформирована) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
ПК-1,2	Доклад в форме презентации	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 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). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

ПК-1,2	Лабораторная работа	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Например: 1. Оформление в соответствии с требованиями (1 балл). 2. Выбор методов измерений и вычислений (1 балл). 3. Умение применять выбранные методы (1 балл). 4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла). Максимальная оценка – 5 баллов.

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 докладов в презентационной форме (вариант 2):

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.

Примерная тематика (контрольных заданий) задач для выполнения:

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

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.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается

определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных

специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

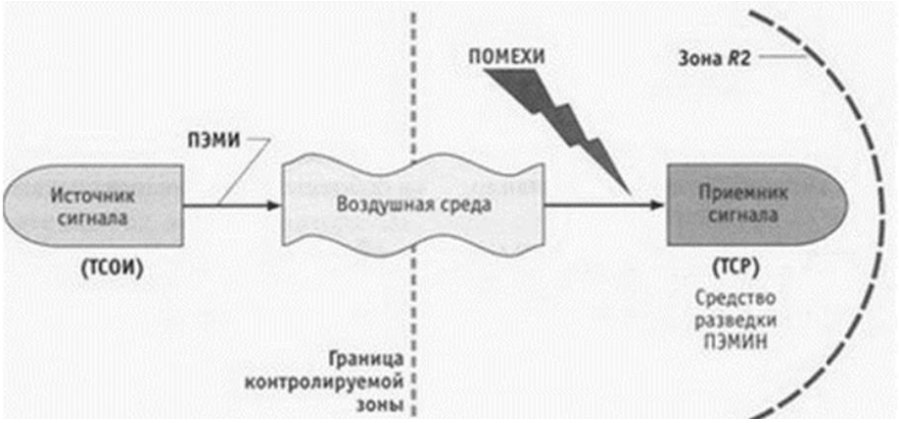

Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

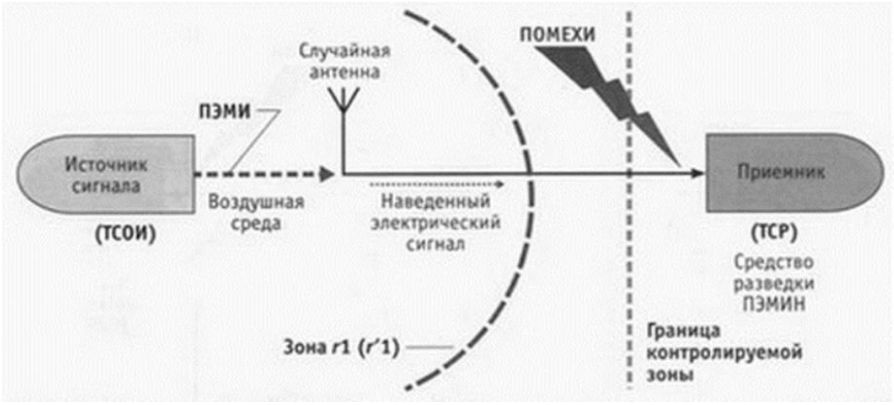

Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

1) Дайте определение специальным исследованиям в рамках данного учебного занятия.

2) Какие и сколько существует грифов секретности в рамках законодательства РФ?
3) Что такое зона r1(r’1) в ТЗИ?
4) Дайте определение ОТСС и ВТСС и в чем их различие?
5) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

1) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
2) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

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

Формой контроля знаний по дисциплине 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	ПК-1,2	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***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%***
Согласно учебному плану	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***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%***
Соглас	Зачет	ПК-1,2	3 вопроса	Зачет	Результаты	Критерии оценки:

но учебному плану				проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	предоставляются в день проведения зачета	**«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 защищенности 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

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

КОМПЛЕКСНЫЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

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

Образовательные технологии**:** ***беседа.***

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

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

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

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

Образовательные технологии: *практическая работа в группах.*

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

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

Образовательные технологии: *групповая дискуссия.*

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

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 и 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: *практическая работа в группах.*

Практическое занятие 6.

Учебные вопросы

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

Продолжительность занятия: 1 ч.

Тема 8. Проведение аттестация объектов информатизации (ОИ)

Вид практического занятия: занятие в смешанной форме

Образовательные технологии: *беседа.*

Практическое занятие 7.

Учебные вопросы

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

8. 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: *групповая дискуссия.*

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.

9.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: *беседа.*

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: *практическая работа в группах.*

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: *беседа.*

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: *групповая дискуссия.*

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: *практическая работа в группах.*

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

Цель и задачи выполнения лабораторных работ: Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

Лабораторная работа 1. ***Использование классических криптоалгоритмов подстановки для защиты текстовой информации***

Цель работы: изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

Учебные вопросы

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:
   - просмотреть предварительно созданный с помощью редактора свой текстовый файл;
   - выполнить для этого файла шифрование;
   - просмотреть в редакторе зашифрованный файл;
   - просмотреть гистограммы исходного и зашифрованного текстов;
   - описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование

- расшифровать зашифрованный текст:
  - с помощью программы, после чего проверить в редакторе правильность расшифрования.
  - вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов и полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

3. Для одноалфавитного метода с задаваемым смешением (шифр Цезаря) следует:
   - выполнить шифрование с произвольным смещением для своего входного текста;
   - просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
   - расшифровать текст с помощью программы;
   - дешифровать зашифрованный шифром Цезаря текст с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
4. Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

   Дешифруйте файл:
   - вручную (объясните ваши действия);
   - с помощью программы.
5. Для инверсного кодирования (по дополнению до 255):
   выполните шифрование для своего произвольного файла;
   просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
   дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.
6. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.
7. Для многоалфавитного шифрования с ключом фиксированной длины:

- выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;
- выполните шифрование и расшифрование для файла произвольного текста;
- просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7.
9. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем.

Примечание: по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия: 2 час

Лабораторная работа № 2 ***Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей***

Цель работы: изучение методов шифрования/расшифрования перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путем перебора всех возможных ключей.

В лабораторной работе рассматривается способ вскрытия шифра, основанный на переборе всех вариантов ключа. Критерием правильности варианта служит наличие в тексте «вероятного слова». Перебирается множество всех возможных ключей, шифрованный текст расшифровывается на каждом ключе. В получившемся «псевдооткрытом» тексте ищется вероятное слово. Если такого слова нет, текущий текст атакуется и осуществляется переход к следующему ключу. Если такое слово найдено, на экран выводится вариант ключа. Затем перебор ключей продолжается до тех пор, пока не исчерпается все множество вариантов. Возможно обнаружение нескольких ключей, при которых в «псевдооткрытых текстах» имеется вероятное слово.

После завершения перебора необходимо расшифровать текст

найденных ключах. «Псевдооткрытый текст» выводится на экран визуального контроля. Если оператор признает текст открытым, работа по вскрытию заканчивается. Иначе данный вариант ключа бракуется и осуществляется переход к следующему ключу.

Учебные вопросы

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Выполнить настройку программы: выбрать метод шифрования, ввести ключи для всех методов, ввести вероятное слово, осуществить все остальные системные настройки.
3. Для метода замены (одноалфавитного метода):
   - выбрать данный алгоритм в списке доступных методов щифрования:
   - установить необходимое смещение;
   - открыть произвольный файл:
   - просмотреть содержимое исходного файла;
   - выполнить для этого файла шифрование (при необходимости но задать имя зашифрованного файла);
   - просмотреть в редакторе зашифрованный файл;
   - ввести вероятное слово;
   - ввести вероятную длину ключа (кроме метода замены);
   - подобрать ключ;
   - выполнить расшифрование со всеми найденными ключами;
   - найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
   - расшифровать файл исходным ключом;
   - проверить результат.
4. Для метода перестановки:
   - выбрать метод перестановки;
   - в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
   - далее действия полностью соответствуют изложенным в п. 3.
5. Для метода гаммирования:
   - выбрать метод;
   - ввести ключ;
   - полностью повторить п. 3.
6. Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс

шифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

10. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем.

Примечание: по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия 2 час

Лабораторная работа 3. ***Генерация простых чисел, используемых в ассиметричных системах шифрования***

Цель работы: изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

Учебные вопросы

1. Проверить на простоту два произвольных целых числа разрядностью не менее 5.

2. Распределение простых чисел.

2.1. Задан интервал вида [x, x + L]. Вычислить количество *П(x, L)* простых чисел в интервале и сравнить с величиной *L/ln(x).* При каких условиях *П(x, L)/L* близко к 1/ln(x) при заданных x = 2000, L = 500, количество простых чисел для деления 5—15, количество оснований 1—2?

2.2. Найти в интервале (1000, 1000 + 300) все простые числа. Пусть L(i) — разность между двумя соседними простыми числами. Построить гистограмму для *L(i).* Вычислить выборочное среднее Lcpeд. Сравнить с величиной ln(x), где x — середина интервала. Задано: количество простых чисел для деления 5—20, количество оснований 1—3.

2.3. Для заданного набора чисел {k} оценить относительную погрешность формулы для *k-го* простого числа:

p(k) = k/ln(k),k = {10, *15,20,30,35}.*

3. Методы генерации простых чисел.

3.1.В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые k простых.

Расчет производится для всех k <= 10.

3.2.Для интервала (1500, 1500 + 300):

а) рассчитать точное количество *Po* простых чисел в интервале, т.е. при проверке задать только тест на делимость. Количество первых простых чисел для деления определяется из расчета максимальное число для деления равно квадратному корню из максимального значения интервала;

б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество P1, вероятно простых чисел, удовлетворяющих этому тесту;

в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основания ми в тесте Ферма. Вычислить количество *P2* вероятно простых чисел, удовлетворяющих этому тесту. Проанализировать полученные данные.

3.3. Известно, что в заданном интервале имеются числа Кармайкла. Найти их. Варианты интервалов:

(1050, 1050 + 100);

(1700, 1700+ 100);

(2400, 2400 + 100).

4. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта.

Примечание: по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № A50346, CD: Обеспечение безопасности персональных данных № A50346, CD: Защита конфиденциальной информации № A50348, электронное учебное пособие [1].

Продолжительность занятия:2 час

Лабораторная работа 4. ***Электронная цифровая подпись***

Цель работы: ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

Учебные вопросы

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой, изложенными выше. Запустить программу labWork6.exe,

предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.
2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.
3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.
4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.
5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.
6. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта

Примечание: по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

Учебная литература: основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия:2 час

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации	***Подготовка докладов по темам:*** Физические основы формирования технических каналов утечки информации (ТКУИ) .Акустический канал утечки информации. Комплексные системы защиты информации *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

2.	Методика проведения специальных исследований в области защиты речевой информации	***Подготовка докладов по темам:*** Порядок аттестации по требованиям безопасности конфиденциальной информации объекта вычислительной техники. Порядок аттестации по требованиям безопасности конфиденциальной информации защищаемого помещения. Аттестация объектов информатизации. Виды защиты информации. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3	Методика проведения специальных исследований в области акустоэлектрических преобразований	***Подготовка докладов по темам:*** Принципы и методы организационной защиты информации. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях. Лицензирование и сертификация в области защиты информации. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Методика проведения специальных исследований в области побочных электромагнитных излучений	***Подготовка докладов по темам:*** Принципы организации информационных систем в соответствии с требованиями по защите информации. Методы программно-аппаратной защиты информации. Способы и средства защиты информации от утечки по техническим каналам. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

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. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

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

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – **…** страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

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. Перечень основной и дополнительной учебной литературы.

Основная литература:

1.Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
4.Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

6. 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.**

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

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