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.06 «ОРГАНИЗАЦИОННО – ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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: Сухотерин А.И. Рабочая программа дисциплины (модуля): Организационно-правовые механизмы обеспечения информационной безопасности. – Королев МО: «Технологический Университет», 2023

Рецензент: **к.в.н., доцент Соляной В.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	№9 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:

1. Раскрытие основ организационно - правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизм их реализации,
2. Раскрытие понятия и видов защищаемой информации по законодательству РФ и Международным документам, системы защиты государственной тайны, основу правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности.

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

Универсальные компетенции:

- УК-3: Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

Профессиональные компетенции:

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

Основными **задачами** дисциплины являются:

- формирование у студентов знаний по основам правового регулирования отношений в сфере информационной безопасности и организационным мероприятиям по защите информации, а также навыков и умения в применении знаний для конкретных условий.
- развитие в процессе обучения системного мышления, необходимого для решения задач организационно-правовой защиты информации с учетом требований системного подхода.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-3.3. Вырабатывает стратегию сотрудничества, формирует команду для достижения поставленной цели, использует методы эффективного руководства коллективом.
- 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:

- УК-3.2. Формулирует задачи членам команды, применяет эффективные стили руководства командой для достижения поставленной цели, корректирует работу команды с учетом интересов, особенностей

поведения и мнений ее членов, разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.

- 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:

- УК-3.1. Анализирует, проектирует и организует межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели, планирует командную работу, распределяет поручения и делегирует полномочия членам команды.

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

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к 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“, “Защищённые информационные системы“ и компетенциях: ПК-1, 3; УК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Основы теории информационной безопасности», «Методы, организация и проведение научных исследований», «Управление информационной безопасностью», а также имеет связи со следующими дисциплинами программы подготовки магистра: «Компьютерное моделирование информационных процессов и технологий», «Информационно – аналитические системы безопасности», «Методы и средства контроля эффективности защиты информации от утечки по техническим каналам», «Методы и средства защиты информации в системах электронного документооборота» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 3	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**108**	**108**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**94**	**94**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	8	8			
Другие виды контактной работы*	**54**	**54**			
Практическая подготовка	**4**	**4**			
Самостоятельная работа	**8**	**8**			
Курсовые работы (проекты)	+	+			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	-	--			
Вид итогового контроля	Экзамен	Экзамен			

* 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.	Практические занятия, час.	Лабораторные работы, час.	Занятия в интеракт. форме, час.	Пр. подготовка час.	Код компетенций
1	2	3	4	5	5	7
Тема 1. Введение. Содержание основных научных понятий и категорий теории безопасности (организационно – правовой аспект)	1	1	1	1	0.5	УК-3
Тема 2. Угрозы информации. Информация как объект защиты (организационно – правовой аспект)	1	1	1	1	0.5	УК-3
Тема 3. Концептуальные документы в области защиты информации. Основные федеральные нормативные правовые акты. Основные подзаконные акты в области защиты информации (организационно – правовой аспект)	1	1	1	1	0.5	УК-3
Тема 4.Система государственных и отраслевых требований (стандартов) в области защиты информации. Особенности зарубежных стандартов защиты информации (организационно – правовой аспект)	1	1	1	1	0.5	УК-3 ПК-2
Тема 5. ГОСТ Р ИСО/МЭК 15408-2002 – аутентичный вариант общих критериев безопасности информационных технологий (организационно – правовой аспект)	2	2	1	1	0.5	УК-3 ПК-2
Тема 6. Нормативные документы ФСТЭК России (организационно – правовой аспект)	2	2	1	1	0.5	УК-3 ПК-2
Тема 7. Общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Проведение сертификационных испытаний (организационно – правовой аспект)	2	2	-	1	0.25	УК-3 ПК-2

Продолжение табл. 2

1	2	3	4	5	6	7
Тема 8. Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация на региональном и международном уровнях (организационно – правовой аспект)	2	2	0.25	1	0.25	УК-3 ПК-2
Тема 9. Общая характеристика. Концепция Информационной безопасности предприятия и ее содержание. Политика информационной безопасности предприятия (организационно – правовой аспект)	2	2	0.25	1	0.25	УК-3 ПК-2
Тема 10. Служба информационной безопасности предприятия (организационно – правовой аспект)	2	2	0.5	3	0.25	УК-3 ПК-2
Итого:	16	16	8	12	4	

4.2. Содержание тем дисциплины

Тема 1. Введение. Содержание основных научных понятий и категорий теории безопасности (организационно – правовой аспект).

Понятия «опасность» и «безопасность». Угрозы, риски, вызовы. Причины и последствия угроз безопасности. Система обеспечения безопасности.

Тема 2. Угрозы информации. Информация как объект защиты (организационно – правовой аспект).

Информация, ее виды и ценность. Основные определения сферы защиты информации. Обеспечение безопасности информации.

Общая характеристика технических каналов утечки информации. Обзор и классификация угроз информации, обрабатываемой СВТ и АС. Основные способы реализации угроз информации. Компьютерные атаки и вирусы. Оценка и анализ незаконно добытой информации.

Тема 3. Концептуальные документы в области защиты информации.

Основные федеральные нормативные правовые акты. Основные подзаконные акты в области защиты информации (организационно – правовой аспект).

Общие положения. Доктрина информационной безопасности России. Концепция использования информационных технологий. Перечень нормативных правовых актов. Федеральный закон «Об информации, информационных технологиях и защите информации». Закон РФ «О государственной тайне». Федеральный закон «О коммерческой тайне». Федеральный закон «О лицензировании отдельных видов деятельности». Федеральный закон «О техническом регулировании». Законы, касающиеся интеллектуальной собственности. Положение Гражданского кодекса РФ по

защите информации. Правонарушения и преступления в информационной сфере. Указы Президента РФ. Постановления Правительства РФ. Ведомственная нормативная база.

Тема 4. Система государственных и отраслевых требований (стандартов) в области защиты информации. Особенности зарубежных стандартов защиты информации (организационно – правовой аспект).

Система государственных и отраслевых требований (стандартов) в области защиты информации. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Общие критерии безопасности информационных технологий.

Тема 5. ГОСТ Р ИСО/МЭК 15408-2002 – аутентичный вариант общих критериев безопасности информационных технологий (организационно – правовой аспект).

Общая характеристика. Введение и общая модель. Функциональные требования безопасности. Требования доверия к безопасности.

Тема 6. Нормативные документы ФСТЭК России (организационно – правовой аспект).

Общая характеристика. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД. Показатели защищенности средств обработки информации.

Тема 7. Общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Проведение сертификационных испытаний (организационно – правовой аспект).

Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия: общие положения; декларирование соответствия; обязательная сертификация. Принципы проведения сертификационных испытаний. Документы сертификационных испытаний.

Тема 8. Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация на региональном и международном уровнях (организационно – правовой аспект).

Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация: в странах СНГ; в Евросоюзе; на международном уровне.

Тема 9. Общая характеристика. Концепция информационной безопасности предприятия и ее содержание. Политика информационной безопасности предприятия (организационно – правовой аспект).

Концепция безопасности предприятия и ее содержание. Назначение, содержание и структура политики безопасности.

Тема 10. Служба информационной безопасности предприятия (организационно – правовой аспект).

Назначение и функции службы безопасности. Содержание деятельности службы безопасности. Структура службы безопасности. Обязанности сотрудников службы безопасности.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2 к настоящей РП

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Организационно-правовые механизмы обеспечения информационной безопасности» приведена в Приложении 1 к настоящей РП.

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

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

5. Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1.Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (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

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 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.

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-Р3.1».

Рисунок 1. Средство активной защиты от утечек за счет ПЭМИН «Соната-Р3.1»

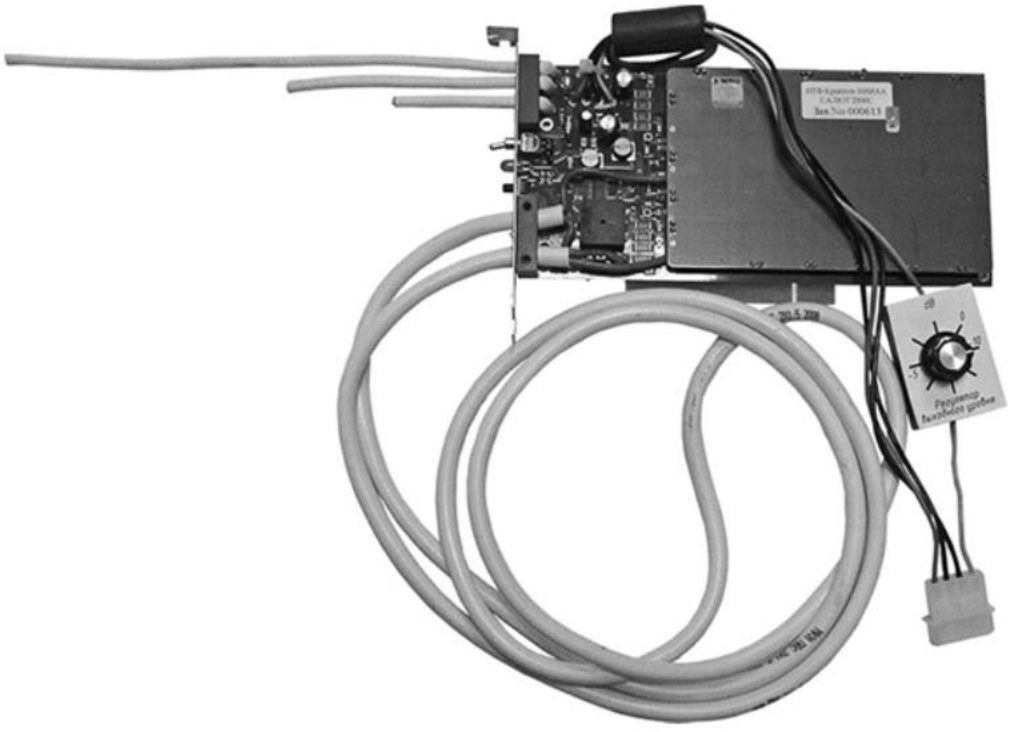
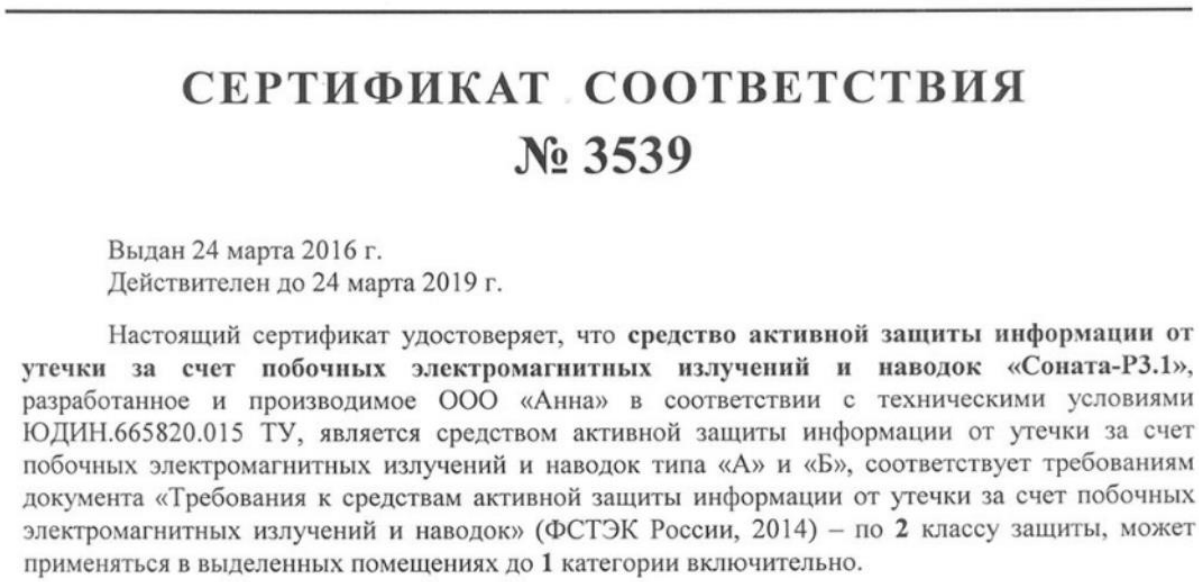


Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»



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).

Таблица 2

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

Диапазон частот, МГц	Вертикальная поляризация, дБ		Горизонтальная поляризация, дБ	
	Без дополнительной антенны	С дополнительной антенной	Без дополнительной антенны	С дополнительной 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?

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
ОРГАНИЗАЦИОННО – ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 формиро-вание компе-тенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	УК-3	Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	Тема: 1-10	-УК-3.3. Вырабатывает стратегию сотрудничества, формирует команду для достижения поставленной цели, использует методы эффективного руководства коллективом.	- УК-3.2. Формулирует задачи членам команды, применяет эффективные стили руководства командой для достижения поставленной цели, корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов, разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.	- УК-3.1. Анализирует, проектирует и организует межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели, планирует командную работу, распределяет поручения и делегирует полномочия членам команды.
3	ПК-2	Способен разрабатывать проектные решения по развитию	Тема: 1-10	- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформление	- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии	- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем,

		автоматизированных ИАС в защищенном исполнении.		м 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***	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-3 ПК-2	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 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.***
УК-3 ПК-2	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств

		сформирована: • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	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.
УК-3 ПК-2	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

УК-3 ПК-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 реферата (доклада):

1. Научные понятия и категорий теории безопасности.
2. Информация как объект защиты.
3. Концептуальные документы в области защиты информации.
4. Особенности зарубежных стандартов защиты информации.
5. Система государственных и отраслевых требований в области защиты информации.
6. Нормативные документы ФСТЭК России.
7. Проведение сертификационных испытаний.
8. Сертификация продукции, ввозимой из-за границы.
9. Концепция Информационной безопасности предприятия и ее содержание.
10. Служба информационной безопасности предприятия.

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

Формой контроля знаний по дисциплине «Организационно-правовые механизмы обеспечения информационной безопасности» являются две текущие аттестации в виде тестов и одна промежуточная аттестация в виде зачета в устной форме.

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
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-3 ПК-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%***
Проводится в сроки, установленные графиком образовательного процесса	Тестирование	УК-3 ПК-2	10	Компьютерное тестирование; время отведенное на процедуру -15 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%
Проводится в сроки, установленные графиком образовательного процесса	Тестирование	УК-3 ПК-2	12	Компьютерное тестирование ; время отведенное на процедуру -15 минут	Результаты тестирования предоставляются в день проведения процедуры Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Проводится в сроки, установленные графиком образовательного процесса	Зкзамен	УК-3 ПК-2	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 20 минут на каждого студента	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях;

						«**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы

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.

Типовые вопросы, выносимые на экзамен:

Вопросы к экзамену

1. Понятия «опасность» и «безопасность». Угрозы, риски, вызовы. Причины и последствия угроз безопасности. Система обеспечения безопасности.
2. Общая характеристика технических каналов утечки информации. Обзор и классификация угроз информации, обрабатываемой СВТ и АС. Основные способы реализации угроз информации. Компьютерные атаки и вирусы. Оценка и анализ незаконно добытой информации.
3. Информация, ее виды и ценность. Основные определения сферы защиты информации. Обеспечение безопасности информации.
4. Общие положения. Доктрина информационной безопасности России. Концепция использования информационных технологий. Перечень нормативных правовых актов.
5. Федеральные критерии безопасности информационных технологий.
6. Общая характеристика. Введение и общая модель. Функциональные требования безопасности. Требования доверия к безопасности.
7. Общая характеристика. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД. Показатели защищенности средств обработки информации.
8. Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия: общие положения; декларирование соответствия; обязательная сертификация.

9. Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация: в странах СНГ; в Евросоюзе; на международном уровне.

10. Концепция безопасности предприятия и ее содержание. Назначение, содержание и структура политики безопасности.

11. Назначение и функции службы безопасности. Содержание деятельности службы безопасности. Структура службы безопасности. Обязанности сотрудников службы безопасности.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ОРГАНИЗАЦИОННО – ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель освоения дисциплины «Организационно – правовые механизмы обеспечения информационной безопасности» - Раскрытие основ организационно - правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизм их реализации.

Основными **задачами** дисциплины являются:

- Освоить понятийный арсенал курса;
- Определить специфику подходов различных научных школ в социологии к проживанию жизни, поведению людей;
- Раскрытие понятия и видов защищаемой информации по законодательству РФ и Международным документам, системы защиты государственной тайны, основу правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности;

1. Указания по проведению практических занятий

Тема 1. Введение. Содержание основных научных понятий и категорий теории безопасности (организационно – правовой аспект)

Практическое занятие 1.

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

Образовательные технологии: *беседа*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

1. Управление информационной безопасностью. Комплексная система управления информационной безопасностью.
2. Основные определения и критерии классификации угроз. Основные угрозы доступности.
3. Основные угрозы целостности.
4. Основные угрозы конфиденциальности.
5. Источники угроз.

Продолжительность практического занятия-4 часа

Тема 2. Политика информационной безопасности отдельных структур (объектов, процессов)

Практическое занятие 2.

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 о политике безопасности отдельных структур

Учебные вопросы:

1. Определение политики информационной безопасности
2. Принципы политики безопасности
3. Виды политики безопасности
4. Политики безопасности для
5. Уровни политики безопасности

Продолжительность практического занятия-4 часа

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

Практическое занятие 3.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

1. Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
2. Нормативные акты предприятия по информационной безопасности.
3. Формы правовой защиты информации на предприятии.

Продолжительность практического занятия-4 часа

Тема 4. Основы оценки эффективности управления информационной безопасностью

Практическое занятие 4.

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

1. Метод оценки рисков на основе модели информационных потоков.
2. Расчет рисков по угрозе конфиденциальность.
3. Расчет рисков по угрозе целостность.
4. Методы оценивания информационных рисков.
5. Табличные методы оценки рисков.
6. Разделение рисков на приемлемые и неприемлемые.

Продолжительность практического занятия-4часа

3. Указания по проведению лабораторного практикума

Цель и задачи выполнения лабораторных работ:

Цель: Изучить механизмы регуляторов и их право-применение при анализе объекта ИБ.

Методика *(определяется технологией изучения нормативно-правовых документов регулирующих область ИБ. и выполнения лабораторных работ (заданий) связанных с изучением требований руководящих документов в области ИБ.*

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:

Лабораторная работа № 1.

Тема: Организационно-правовые механизмы. Структура информационных ресурсов и администрирование в компьютерных системах

Цель: Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.

Продолжительность практического занятия-2 часа

Задание.

Тема: «Нормативно-правовая база проведения аудита информационной безопасности организаций».

Продолжительность занятия – 4 академических часа.

Цель лабораторной работы:

Изучение нормативно-правовых и законодательных актов РФ, регулирующих проведение аудита информационной безопасности.

Задачи лабораторной работы:

- закрепление теоретических знаний в области правового обеспечения информационной безопасности;

- исследование терминологической базы;
- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации;
- формирование навыка работы с нормативными документами по исследуемому вопросу.

Задание лабораторной работы:

Используя теоретический материал, подготовить отчёт, включающий ответы на контрольные вопросы.

Шаблон отчёта представлен в Приложении №2.

Учебные вопросы:

1. Правовые вопросы обеспечения информационной безопасности.
2. Доктрина информационной безопасности Российской Федерации.
3. Федеральные законы в области информационной безопасности.
4. Стандарт Банка России СТО БР ИББС-1.0-2014.

Теоретическая часть:

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия этим угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, административного, уголовного и информационного).

Предмет правового обеспечения информационной безопасности опредставляет собой совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз.

Правовые нормы и институты, образующие правовое обеспечение информационной безопасности, закрепляются в нормативных правовых актах, являющихся источниками права в этой области и составляющих соответствующее законодательство.

Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 05.12.2016 г. №646.

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Федеральные законы закрепляют значительное количество норм, регулирующих отношения в области обеспечения информационной безопасности. К числу данных законов относятся Федеральный конституционный закон «О Правительстве Российской Федерации», Федеральный конституционный закон «Об Уполномоченном по правам человека в Российской Федерации», Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Налоговый кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Таможенный кодекс Российской Федерации и др.

Важную роль в правовом регулировании отношений в области обеспечения информационной безопасности играют такие основополагающие нормативные правовые акты, как законы Российской Федерации «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной

инфраструктуры Российской Федерации», «О персональных данных», «Об электронной подписи» и др.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ.

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Федеральный закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации. Закон дает определения терминам, связанным с определением и защитой информации. Описывает классификацию информации, а также порядок государственного регулирования неправомерных случаев распространения информации и помимо этого, регулирует отношения, связанные со сбором и обработкой биометрических данных клиентов банка.

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ.

Принят Государственной Думой 12 июля 2017 года. Одобрен Советом Федерации 19 июля 2017 года.

Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.

Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой органами государственной власти различных уровней, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации.

Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ.

Принят Государственной Думой 9 июля 2004 года. Одобрен Советом Федерации 15 июля 2004 года.

Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Федеральный закон «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ.

Принят Государственной Думой 25 марта 2011 года. Одобрен Советом Федерации марта 2011 года.

Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Федеральный закон «Об аудиторской деятельности» от 30.12.2008 г. № 307-ФЗ.

Принят Государственной Думой 24 декабря 2008 года. Одобрен Советом Федерации 29 декабря 2008 года.

Федеральный закон определяет правовые основы регулирования аудиторской деятельности, особенности саморегулирования в сфере аудиторской деятельности в Российской Федерации.

«Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» СТО БР ИББС-1.2-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399).

Стандартом Банка России СТО БР ИББС-1.0-2014 с целью проверки уровня информационной безопасности как самого Банка России, так и организаций банковской системы Российской Федерации определено требование проведения регулярного аудита ИБ и самооценки ИБ.

Стандарт устанавливает способы определения степени выполнения требований стандарта Банка России СТО БР ИББС-1.0-2014, а также итогового уровня соответствия ИБ требованиям стандарта Банка России СТО БР ИББС-1.0-2014 при проведении аудита ИБ и самооценки ИБ.

Контрольные вопросы:

1. Что такое «правовое обеспечение информационной безопасности» и в чем заключается его предмет?
2. Какой документ представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере?

3. Что понимается под информационной безопасностью согласно Доктрине ИБ РФ?

4. Какие вопросы регулирует Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ?

5. Перечислите принципы обеспечения безопасности критической информационной инфраструктуры согласно Федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ

6. Какова цель Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

7. Раскройте понятия терминов «электронная подпись», «сертификат ключа проверки электронной подписи», «ключ электронной подписи», «ключ проверки электронной подписи», «удостоверяющий центр» согласно Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

8. Что понимается под коммерческой тайной? Какие сведения не могут составлять коммерческую тайну согласно Федеральному закону «О коммерческой тайне» от 29 июля 2004 г № 98-ФЗ?

9. Что регулирует Федеральный закон «Об аудиторской деятельности» от 30.12.2008 № 307-ФЗ? Кем осуществляется правовое регулирование аудиторской деятельности?

10. Цель и задачи «Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» СТО БР ИББС-1.2-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399).

Лабораторная работа № 2.

Тема: Организационно-правовые механизмы. Анализ угроз информационной безопасности

Цель: Изучить механизмы и их право-применение при анализе объекта ИБ. Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.

Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.

Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

Продолжительность практического занятия-2 часа

Задание.

Лабораторная работа

«Исследование каналов утечки через ПЭМИН в персональной ЭВМ»

1. Цель работы

1.1 Исследование способов формирования ПЭМИН каналов утечки КИ, создаваемых устройствами и элементами ПЭВМ.

1.2 Экспериментальное исследование ПЭМИН, создаваемых ВДТ (дисплеями, мониторами ПЭВМ) разного типа (в виде электронно-лучевой трубки – ЭЛТ; жидкокристаллический – ЖК) в области частот 10 кГц ... 1 ГГц.

2. Литература

2.1 Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. М.: Горячая линия – Телеком, 2005. – 416 с.

2.2 Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникаций. М.: ИД «Технологии», 2005. – 320 с.

2.3 Описание тестовой программы ЦБИ «Сервис».

3. Приборы и материалы

Анализатор спектра: ROHDE & SHWARZ FS300.
Персональный компьютер: Pentium (Celeron) IV.
Монитор ЭЛТ 15", 17" в составе ПЭВМ.
Монитор ЖК (LCD) 15", 17" в составе ПЭВМ.
Активная измерительная дипольная антенна АИ5-0.
Активная измерительная рамочная антенна АРА-2.
USB-Flash drive память (USB накопитель).

4. Подготовка к работе

4.1. Ознакомиться с основными правилами работы с прибором ROHDE&SHWARZ FS300 (см. приложение 2; руководство по эксплуатации анализатора спектра R&S®FS300). Обратить внимание на процедуру сохранения графической копии экрана на внешнюю USB-Flash drive память.

4.2. Ознакомиться с возможностями и порядком применения тестовой программы ЦБИ «Сервис».

4.3. Сделать предварительный расчет прогнозируемых сигналов ПЭМИН по программе ZEBRA ЦБИ «Сервис», используя частоты разверток заданного типа ВДТ (далее – монитора) ПЭВМ. Тип монитора и параметры разрешения его экрана задаются преподавателем.

4.4. Получить у преподавателя допуск к работе.

5. Описание измерительной установки

5.1. Структурная схема измерительного стенда представлен на рис. 1.

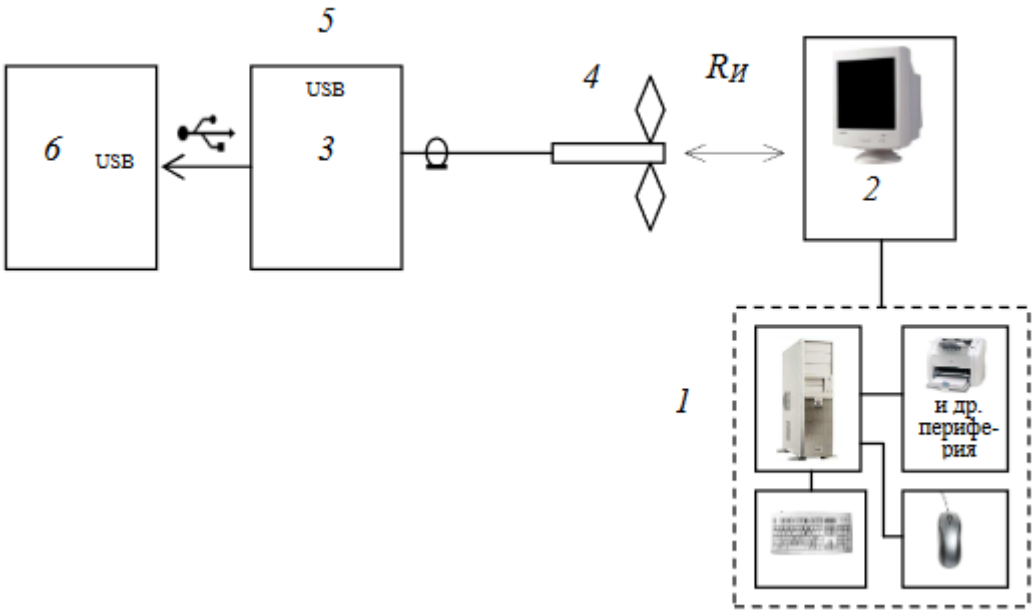


Рис. 1 Измерительный стенд

1 – Персональный компьютер ПК1.
2 – Монитор (ЭЛТ, ЖК) ПЭВМ
3 – Анализатор спектра ROHDE & SHWARZ FS300 (далее R&S FS300).
4 – Измерительная антенна АИ5-0.
5 – USB-Flash drive память (накопитель).
6 – Персональный компьютер ПК2. и др. периферия

6. Выполнение работы

6.1. Включить питание ПК1; ПК2 и анализатора R&S FS300. При необходимости использования программы FS-300-K1 соединения анализатора спектра R&S FS300 с ПК2 (см. рис. 1), дождаться загрузки операционных систем в течение 1-5 мин. Включить питание активной измерительной антенны АИ5-0.

6.2. Собрать (проверить сборку) схему измерения ИМ-составляющих сигналов ПЭВМ согласно рис. 1. Подключить сигнальные кабели, USB-Flash drive накопитель 5 в соответствующие гнезда. Установить расстояние RИ между измерительной антенной 4 и монитором 2 в соответствии с заданием преподавателя.

6.3. Настроить анализатор спектра R&S FS300 на отображение частот сигнала ПЭМИН, рассчитанных предварительно согласно п. 4.3. Первоначально полосу отображаемых на экране частот SPAN установить равной 1000 МГц, остальные настройки анализатора оставить «по умолчанию». В дальнейшем, при уточнении частот сигналов ПЭМИН, полосу SPAN устанавливают в диапазоне 100-1000 МГц по наилучшему наблюдению исследуемого сигнала.

6.4. Установить опции анализатора «SYS» на сохранение графической копии экрана во внешнюю USB-Flash drive память, либо запустить и настроить программу связи анализатора спектрас ПК FS300-K1 (см. приложение 3).

6.5. Установить с помощью программы «IVT BlueSoleilTM» беспроводное соединение между ПК1 и ПК2 (см. приложение 4). Используя профиль передачи файлов (File Transfer Profile – FTP), задать копирование заранее подготовленного (с любым тестовым содержанием) файла объемом 10-50 Мб с одного ПК на другой, контролируя данный процесс по индикатору на ПК.

6.6. Запустить на ПК1 тестовую программу разработки ЦБИ
«Сервис» WinVideo: - краткая справка по работе с программой вызывается с помощью клавиши F1 на ПК1; - для работы программы выбирается режим «Вкл. / Выкл. экрана –

Вручную»: после этого при нажатии на кнопку клавиатуры «SPACE» на экране монитора либо отображаются вертикальные полосы тестового сигналов, либо экран гаснет. Тестовый сигнал представляет собой чередование черных и белых полос на экране монитора. Для разных мониторов и при различных разрешениях экрана их число неодинаково. В таблице 1. указано число полос в соответствии с порядком их вывода на экране монитора ПЭВМ. Число полос тестового сигнала можно изменять с помощью клавиш «←» и «→» на клавиатуре ПК.

Порядок появления на мони-торе	Число полос			
	ЭЛТ монитор 800×600	ЭЛТ монитор 1024×768	ЖК монитор 800×600	ЖК монитор 1024×768
1	2	2	2	2
2	4	4	4	4
3	8	8	8	8
4	10	16	10	16
5	16	32	16	32
6	20	64	20	64
7	32	128	32	128
8	40	256	40	256
9	50	512	50	512
10	80	1024	80	1024
11	100		100	
12	160		160	
13	200		200	
14	400		400	
15	1000		1000	

Таблица 1. Параметры выводимых тестовых изображений

При включенном мониторе 2 на экране анализатора R&S FS300 наблюдается суммарный спектр сигнала эфирного фона по ЭМИ и ПЭМИН, полученный с помощью измерительной антенны 4 в заданной полосе частот. При выключенном мониторе 2 экран анализатора R&S FS300 демонстрирует спектр сигналов эфирного фона в месте измерения.

6.7. Снять спектрограммы сигналов в полосе частот 10 кГц ... 1 ГГц при помощи анализатора R&S FS300 и измерительной антенны 4 при следующих исходных данных:

- ЭЛТ-монитор с разрешением экрана 800×600 пиксельных точек

Число полос тестового сигнала 80 200 1000

Обратить внимание на область частот 80 ... 200 МГц.
- ЭЛТ-монитор с разрешением экрана 1024×768 пиксельных точек
Число полос тестового сигнала 8 32 256
Обратить внимание на область частот 80 ... 800 МГц.
- ЖК-монитор с разрешением экрана 800×600 пиксельных точек
Число полос тестового сигнала 80 200 1000
Обратить внимание на область частот 100 ... 850 МГц.
- ЖК-монитор с разрешением экрана 1024×768 пиксельных точек
Число полос тестового сигнала 8 32 256
Обратить внимание на область частот 120 ... 900 МГц.
6.8. Для снятия спектрограмм необходимо выполнить следующие действия:
- зафиксировать частоты, на которых сигналы ПЭМИН по уровню заметно превышают сигналы шума. Различие между ними проще выявить путем наложения на экране R&S FS300 двух спектрограмм: при погасшем экране ПЭВМ и экране с полосами, сформированными тестовой программой WinVideo;
- для снятия спектрограмм используется USB-накопитель, который устанавливается в USB-разъем на задней стенке анализатора спектра (см. приложение по работе с R&S FS300).

При снятии спектрограмм сигналов ПЭМИН возможно использование программы соединения анализатора спектра R&S FS300 с ПК: FS-300-K1.

6.9. Сохранить графическую копию экрана R&S FS300 на внешнюю USB-Flash drive память, используя системные функции (кнопка «SYS» на анализаторе спектра) меню «FILE». Либо сохранить копию экрана на жесткий диск ПК2, используя программу связи FS300-K1.

6.10. Вывод на экран R&S FS300 двух спектрограмм позволяет наглядно фиксировать сигналы ПЭМИН на фоне посторонних (фоновых, помеховых, шумовых) сигналов. Функция «TRACE» позволяет выбирать активную в данный момент кривую на экране(подробности см. в приложениях 2 и 3).

7. Обработка результатов измерений

7.1. Для составления отчета по лабораторной работе необходимо обработать спектрограммы сигналов и, в соответствии с п. 6.8, выявить на них частоты, где обнаружены составляющие ПЭМИН, заметно превышающие уровень фона по ЭМИ. Полученные данные следует свести в таблицу 7.2.

7.2. На рис. 7.1-7.2. представлены ожидаемые спектрограммы сигналов ПЭМИН на примере ЭЛТ-монитора с разрешением 800×600 точек. На рис. 1-2 используются обозначения: F – частота сигнала ПЭМИН, в МГц; ΔP – превышение уровня сигнала ПЭМИН над уровнем фона по ЭМИ, шумов и помех, в дБм.

Число полос тестового сигнала	80	200	макс
Частоты, на которых обнаружен сигнал ПЭМИН, МГц	87,7	192	

Таблица 2. Результаты измерений

7.3. Сделать выводы по результатам проделанной работы, указав, при каких мониторах, в каких режимах работы ПЭВМ и при разрешениях уровни ПЭМИН здесь наиболее заметны.

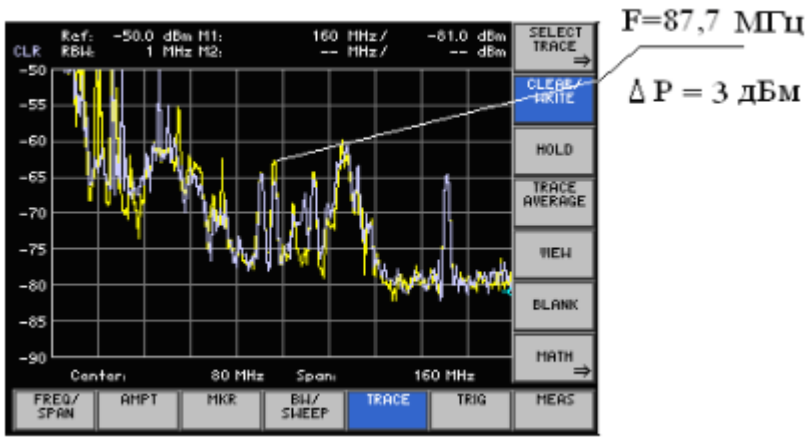


Рис. 2. Спектрограмма сигнала ПЭМИН с числом полос тестового сигнала 80

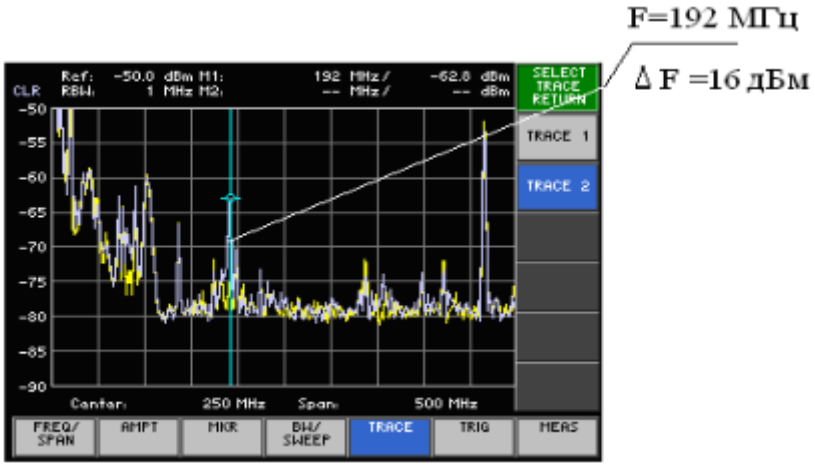


Рис. 3. Спектрограмма сигнала ПЭМИН с числом полос тестового сигнала 200

8. Содержание отчета

В отчете необходимо привести:

- формулировку цели и задания на выполнение работы;
- схему лабораторной установки; - список приборов и оборудования;
- данные предварительных расчетов;
- копии экрана анализатора R&S FS300 со спектрограммами сигналов ПЭМИН;
- выводы по результатам выполненных исследований.

Лабораторная работа № 3.

Тема: Организационно-правовые механизмы. Основные уровни защиты информации в компьютерных системах

Цель: Изучить механизмы и их право-применение при анализе объекта ИБ. Методы и средства обеспечения защиты информации в компьютерных системах. Защита представления информации. Защита содержания информации.

Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.

Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок. Аппаратные средства защиты в КС. Задачи, решаемые программными средствами защиты.
Продолжительность практического занятия-2 часа
Задание.

Тема: **Нормативное регулирование и обеспечение кибербезопасности в организациях кредитно-финансовой сферы.**

Цель занятия: **Анализ нормативных документов по защите информации в российской кредитно-финансовой сфере.**

Продолжительность занятия **– 4 академических часов.**

Задание:

Результаты выполнения каждого задания необходимо записать в отчет.

1. Определить статьи, непосредственное посвященные защите информации в Конституции Российской Федерации;
2. Ознакомиться с основными терминами и определениями Концепции национальной безопасности РФ;
3. Ознакомиться с основными терминами и определениями Доктрины информационной безопасности РФ;
4. Привести перечень федеральных законодательных актов, регулирующих защиту информации (3 и более);
5. Привести перечень указов президента или постановлений совета министров правительства РФ, регулирующих защиту информации (3 и более);
5. Привести перечень Государственных технических стандартов (ГОСТ), регулирующих защиту информации (5 и более);
6. Определить статьи, непосредственное посвященные защите информации в Кодексе Российской Федерации об административных правонарушениях;
7. Привести перечень требований и условий при осуществлении деятельности по технической защите конфиденциальной информации (4 и более);

Ссылки на материалы для выполнения лабораторной работы

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. Концепция национальной безопасности РФ (в ред. Президента РФ от 10.01.2000 N 24)
3. Доктрина информационной безопасности РФ
4. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022)

Лабораторная работа № 4.

Тема: Организационно-правовые механизмы. Основные положения формальной теории защиты информации

Цель: Изучить механизмы и их право-применение при анализе объекта ИБ. Концепция монитора безопасности обращений в КС.

Правила разграничения доступа субъектов к объектам в ОС.

Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО

Продолжительность практического занятия-2 часа

Задание

Тема: *Оптико-электронный канал утечки информации.*

Цель занятия: *Определить необходимость наличия организационно-технических мер для противодействия утечкам информации через оптико-электронный канал.*

Продолжительность занятия – *4 ак.ч.*

Задание –

1. Изучить методы и средства снятия информации по оптико-электронному каналу утечки;

2. Изучить методы и средства защиты информации от утечки по оптико-электронному каналу;

3. Создать лазерное средство съема информации;

4. Проверить эффективность созданного средства;

5. Оформить отчет по результатам испытаний с указанием:

-эффективной дальности;

-процентом разборчивости речи;

-влиянием внешних условий на качество принимаемой информации;

-выводом о необходимости и целесообразности применения организационно-технических мер для защиты информации от утечки по данному каналу.

Данные для выполнения лабораторной работы представлены в Приложении.

Приложение 1

Методы и средства снятия информации по оптико-электронному каналу утечки

Хотя добыча информации происходила и раньше, документированная история шпионажа насчитывает несколько веков. С технологическим развитием человечества у корпораций и государств появляется все больше методов и средств для добычи информации, обнаруживаются новые каналы утечки информации. Но в настоящее время то, что было доступно только на высшем уровне (спецслужбы, международные компании) из-за своих сложности исполнения, доступности и стоимости, с развитием технологий стало доступным более широкому кругу лиц, стало коммерческим продуктом.

Одним из известных каналов утечки информации является оптико-электронный. В настоящее время в действующих руководящих и методических документах Российской Федерации по защите конфиденциальной информации оптико-электронный канал утечки информации не рассматривается, поэтому требований для закрытия данного канала при разработке систем для обеспечения защиты информации нет. В данной статье рассмотрены виды лазерных микрофонов, применяющихся в качестве систем акустической разведки, и их развитие.

В первую очередь необходимо описать принцип действия утечки информации через данный канал. Акустический речевой сигнал, распространяясь в воздушной среде, воздействует на поверхности помещения (в том числе отражающие, например, оконные стекла, зеркала и т.п.) и предметов, которые в нем находятся и вызывает вибрацию этих поверхностей. С помощью специального оборудования (лазерных микрофонов) вибрирующие отражающие поверхности облучаются лазерным лучом, отраженное лазерное излучение которого модулируется по фазе и амплитуде и принимается приемником лазерного микрофона. При демодуляции принятого излучения выделяется речевая информация (рис.1).

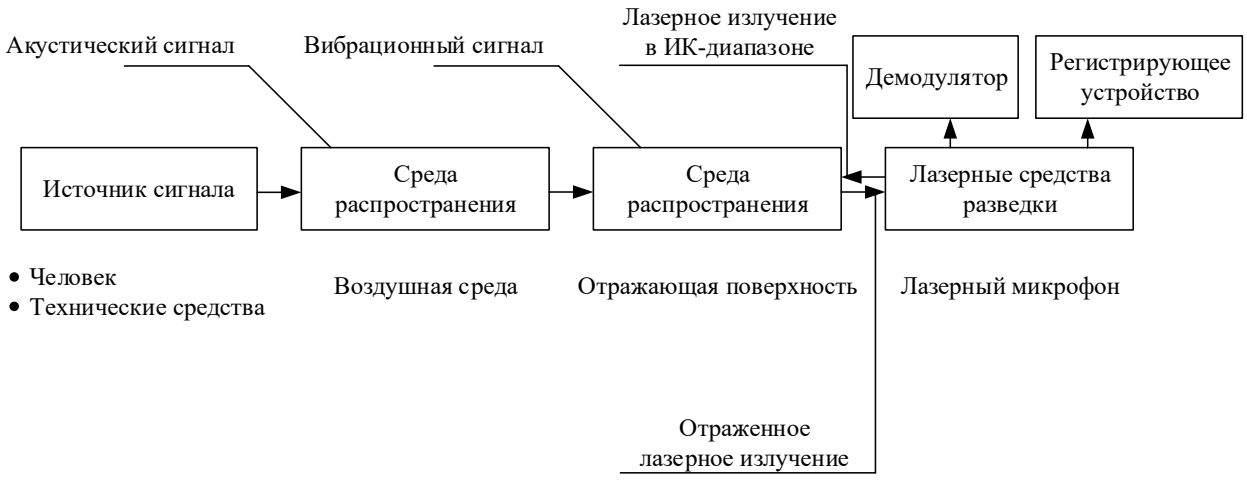


Рисунок 1 – Схема утечки информации через оптико-электронный канал

В первых системах акустической разведки вместо лазеров использовался инфракрасный луч. Одной из первых разработок систем

акустической разведки, являющейся разновидностью лазерных микрофонов, считается «Буран». Принцип действия и считывания информации с отражающих поверхностей помещения аналогичен описанному выше, но в качестве лазера использовалось инфракрасное излучение. Изобретателем системы является советский ученый Лев Сергеевич Термен. Данная система была эффективной на расстоянии до 500 м., но в случае дождя или тумана не работала должным образом. Полученный сигнал проходил обработку с помощью аналоговых технологий, доступных в то время. Также в то время существовала практика внедрения в стекло окна миниатюрных призм, почти невидимых для обычного взгляда, для улучшения чувствительности лазера и помощи в его позиционировании. Так как в подавляющем большинстве случаев системы для ведения разведки применяются спецслужбами государств, доказательства и факты их применения редко придаются огласке, а многие из тех, что существуют на данный момент нельзя однозначно подтвердить или опровергнуть.

Рассмотрим различные варианты исполнения и использования подобных систем.

В общем виде лазерный микрофон состоит из лазера, приемника и демодулятора (рис. 2). Луч лазера падает под некоторым углом на стекло окна, которое под воздействием акустического речевого сигнала создает вибрацию. Отраженный луч модулируется и принимается приемником, далее производится демодуляция, при которой выделяется речевая информация. Система довольно проста в своем исполнении, но требует тщательной настройки.

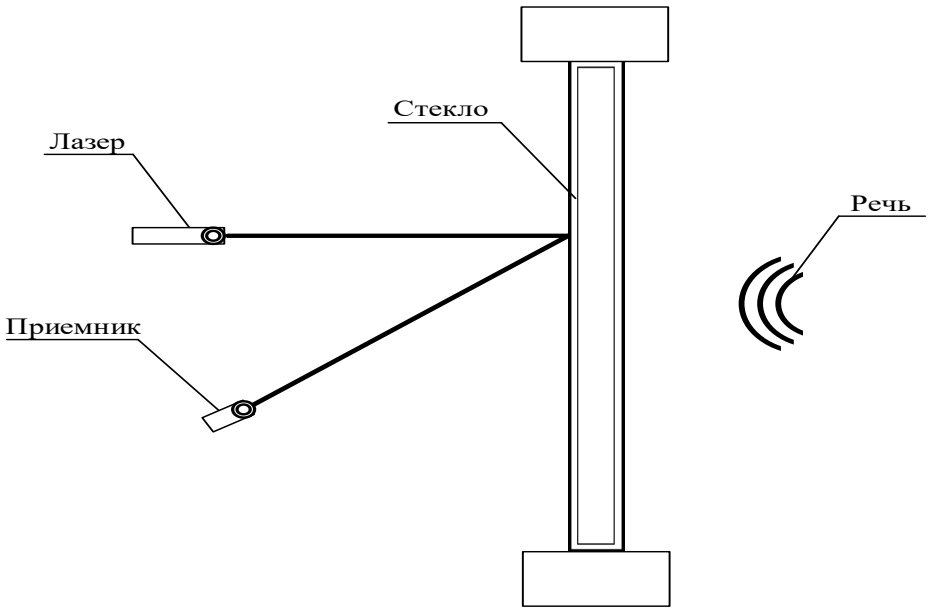


Рисунок 2 – Принцип действия лазерного микрофона

Данную систему можно улучшить с помощью сплиттера (делителя). Он необходим для повышения чувствительности системы. Его применение позволяет совместить приемник с лазером, для сведения падающего и отраженного луча в одну точку (рис. 3).

Возможно создание любительских систем из комплектующих и элементной базы, находящихся в свободном доступе. Конечно, качество таких систем (чувствительность, дальность, качество передаваемой информации), по сравнению с профессиональным оборудованием, будет невелико, но они могут дать общее представление о функционировании лазерных микрофонов, и в каких-то случаях вероятно их использование.

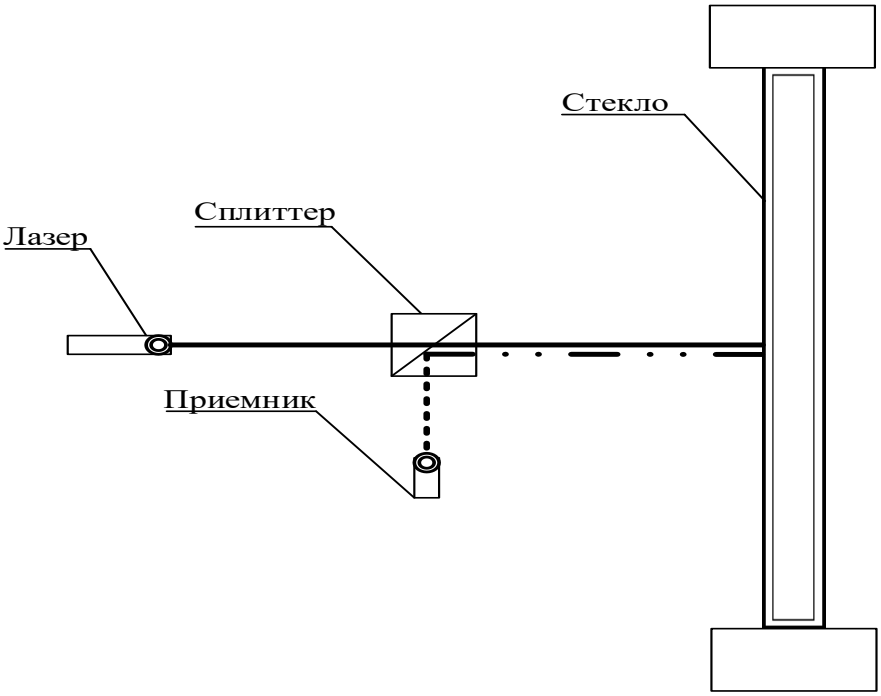


Рисунок 3 – Лазерный микрофон с применением сплиттера

Можно получить еще более высокую чувствительность, чем в предыдущей схеме если использовать интерферометрию (рис.4). Данный подход имеет несколько недостатков. Наиболее бросающийся в глаза – большие различия в длине плеча. В идеале оба плеча должны быть одинаковой длины. При этом способе многократно возрастает сложность настройки, так как отраженные лучи должны приниматься согласованными по фазе, если этого не происходит, то интерференционная картина смазывается или вообще отсутствует, и это приводит к падению чувствительности.

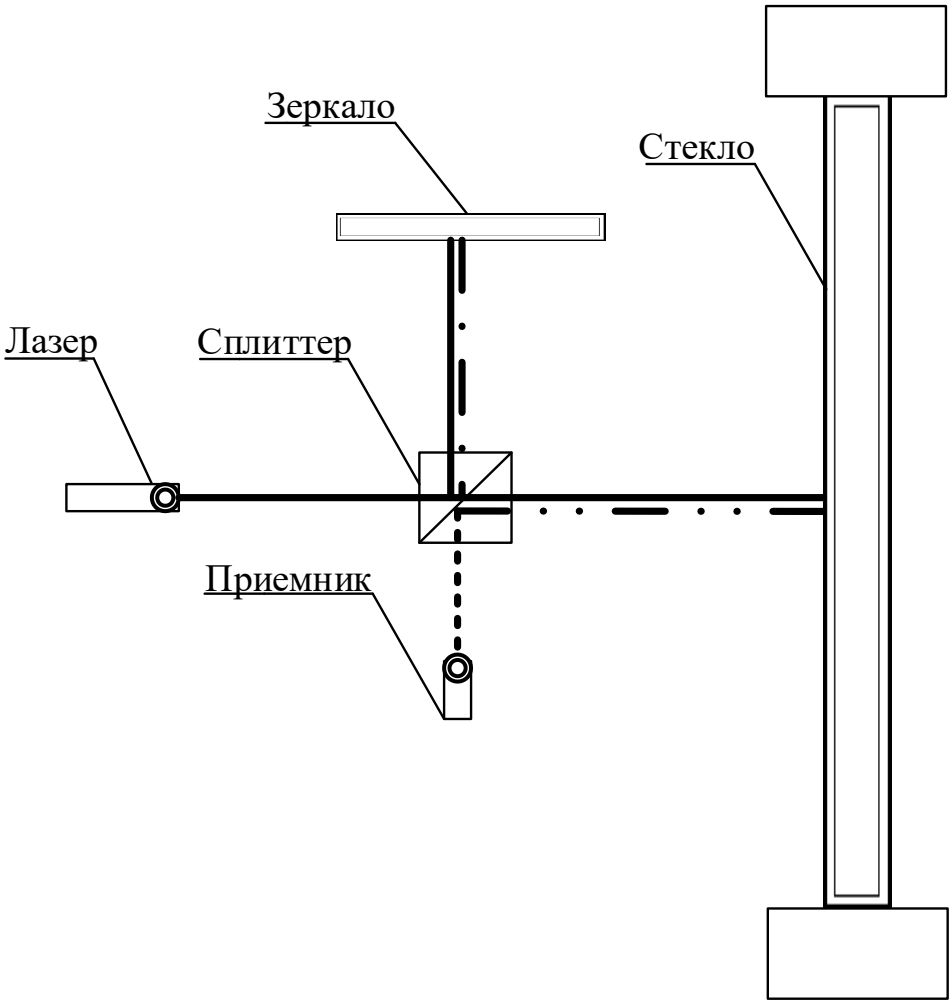


Рисунок 4 – Использование интерферометрии в лазерных микрофонах

Наиболее совершенный вариант исполнения – интерферометр, с плечами равной длины (Dual Beam Laser Mic) (рис.5). В этом исполнении лазерного микрофона применяется дифференциальный метод измерения акустической вибрации. Информация снимается с малоразмерной секции стекла, вследствие чего сильно ослабляется синфазная помеха, вызываемая низкочастотными колебаниями стекла.

Очевидно, что создание любительских систем в данном исполнении маловероятно в виду сложности и отсутствия некоторых компонентов в свободном доступе. Принципиальные схемы профессиональных систем лазерной акустической разведки невозможно найти в открытом доступе, в виду тематики использования устройств, но можно предположить, что по крайней мере ранние модели работали по схожему принципу действия.

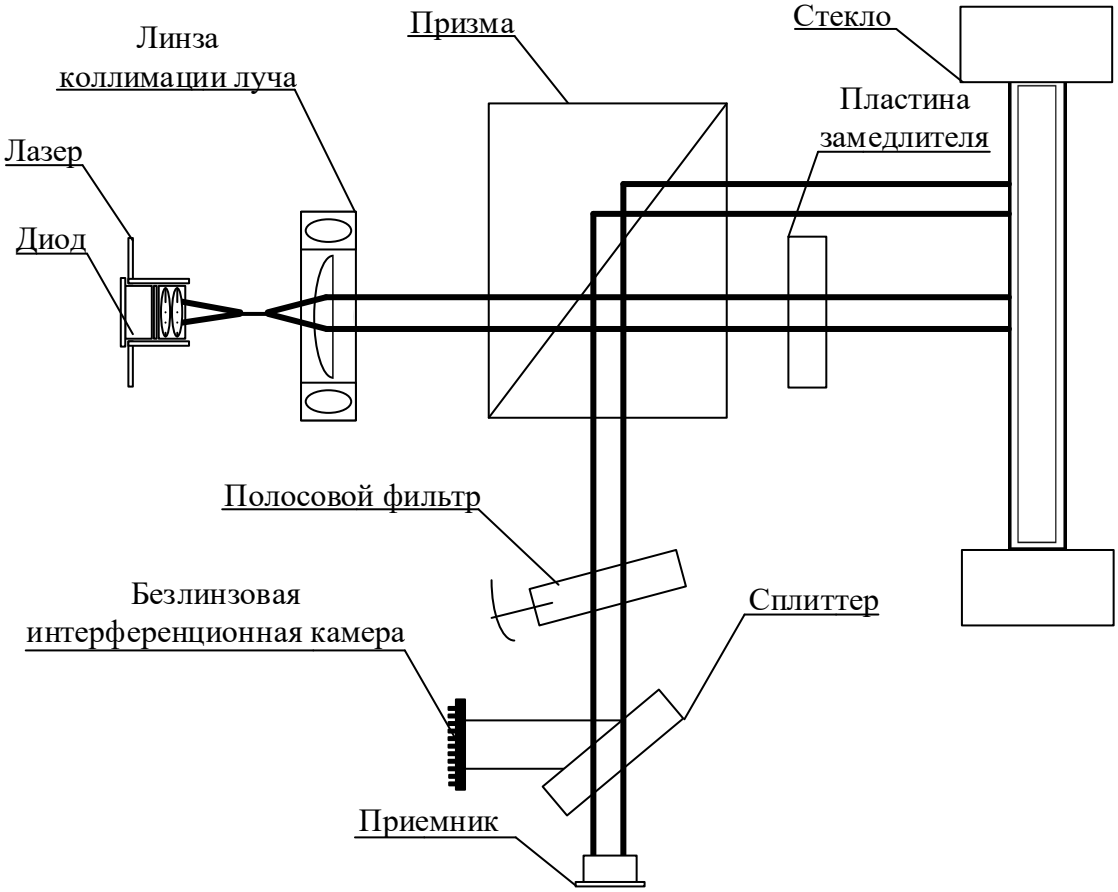


Рисунок 5 – Интерферометр

Технические характеристики и надежность лазерных систем акустической разведки улучшаются с развитием лазерных технологий. При анализе данных из открытых источников, где указаны характеристики лазерных микрофонов (табл. 1) было выявлено, что максимальная дальность работы устройств – 1000 м., но при этом стоит учитывать, что испытания проводились в идеальных условиях.

Таблица 1 – Существующие модели лазерных микрофонов

Модель	Производитель	Страна	Сайт	Дальность
SIM-LAMIC	SIM Secure Information Management	Германия	sim-secure.de	500
Laser-3000	PKI Electronic Intelligence	Германия	pki-electronic.com/	500
Laser-3500	PKI Electronic Intelligence	Германия	pki-electronic.com/	500
HP-150	Hewlett-Packard	США	hp.com	1000
LAS-MIC	Endoacustica	Италия	endoacustica.com	800

На качество полученной информации влияет множество факторов, таких как:

1. Характеристики применяемого лазера:
- Рабочая длина волны лазерного излучения
- Выходная мощность (интенсивность)
- Синфазность

2. Характеристики применяемого приемника:
- Спектральная чувствительность
- Избирательность по длинам волн

3. Качество поверхности

4. Погодные условия:
- Ветер
- Грязь
- Туман
- Дождь

5. Уровень акустических шумов

6. Уровень источника сигнала

Рассмотрим преимущества и недостатки лазерных систем акустической разведки.

Преимущества:
- Сложность выявления канала утечки
- Высокая дальность
- Применение в системе защиты информации организации мер, направленных на закрытие оптико-электронного канала маловероятно.

Недостатки:
- Высокая стоимость систем
- Зависимость от множества внешних факторов
- Развертывание системы требует высококвалифицированного специалиста

Стоит заметить, что новейшие лазерные микрофоны (табл. 2), называемые оптоакустическими, имеют меньшую паспортную максимальную дальность чем свои предшественники. Но при этом они лишены многих недостатков, присутствующих в предыдущих моделях, а также обладают значительными преимуществами.

Таблица 2 – Оптоакустические лазерные микрофоны

PKI 2510	PKI Electronic Intelligence	Германия	pki-electronic.com/	150
PKI 3100	PKI Electronic Intelligence	Германия	pki-electronic.com/	300
OAM-2000	SIM Secure Information Management	Германия	sim-secure.de	300

Отличия новейших лазерных микрофонов от старых моделей:

- Позволяют снимать информацию через окно или небольшое отверстие с предметов, находящихся внутри помещения
- Не зависят от угла падения луча
- В оптическом блоке размещены излучатель и приемник, что облегчает управление
- Окружающие шумы между датчиком и целью не влияют на качество передачи информации
- Работают при минимальных вибрациях поверхностей

Чтобы обеспечить защищенность организации от утечки информации с помощью лазерных микрофонов применяется комплекс организационных и технических мер. Технические меры подразумевают использование активных и пассивных средств защиты для воздействия на канал перехвата информации.

Организационные меры включают в себя:

- использование погодных условий
- проведение переговоров в помещениях, обеспечивающих за их пределами наибольший уровень фонового шума
- проведение переговоров в помещениях, где отсутствуют окна (подвальные помещения и т.п.)
- использование помещений, в которых расстояние до границ контролируемой зоны превышает радиус действия средств разведки

Технические меры включают в себя:

- применение активных средств акустической защиты
- применение ставней, экранов на окнах, виброштор

Новые модели лазерных микрофонов (оптоакустические) отличаются от старых моделей предыдущего поколения. Направленные лазерные микрофоны фокусировались на преломлении лазерного луча от оконного стекла, тогда как новые модели, к примеру, проницают его, нацеливаясь на предметы внутри помещения. Таким образом установки вибровозбудителей на окна недостаточно для защиты помещения от оптоакустических лазерных

микрофонов, необходим комплексный подход с применением вибровозбудителей, экранов (ставней, виброштор).

Методы и средства защиты информации от утечки по оптико-электронному каналу

На рынке существуют как сертифицированные, так и несертифицированные решения в различном исполнении. У каждого вида решения есть свои плюсы и минусы. Рассмотрим данные решения с точки зрения проектирования системы защиты информации, ее внедрения и повседневной эксплуатации.

Первый вариант. Готовые средства защиты информации, предназначенные для монтажа на элементы интерьера (внутренние рольставни, металлические жалюзи). В составе блок управления и акустические излучатели, вибровозбудители. Схема монтажа средств защиты информации на металлические жалюзи приведена на рис. 2.

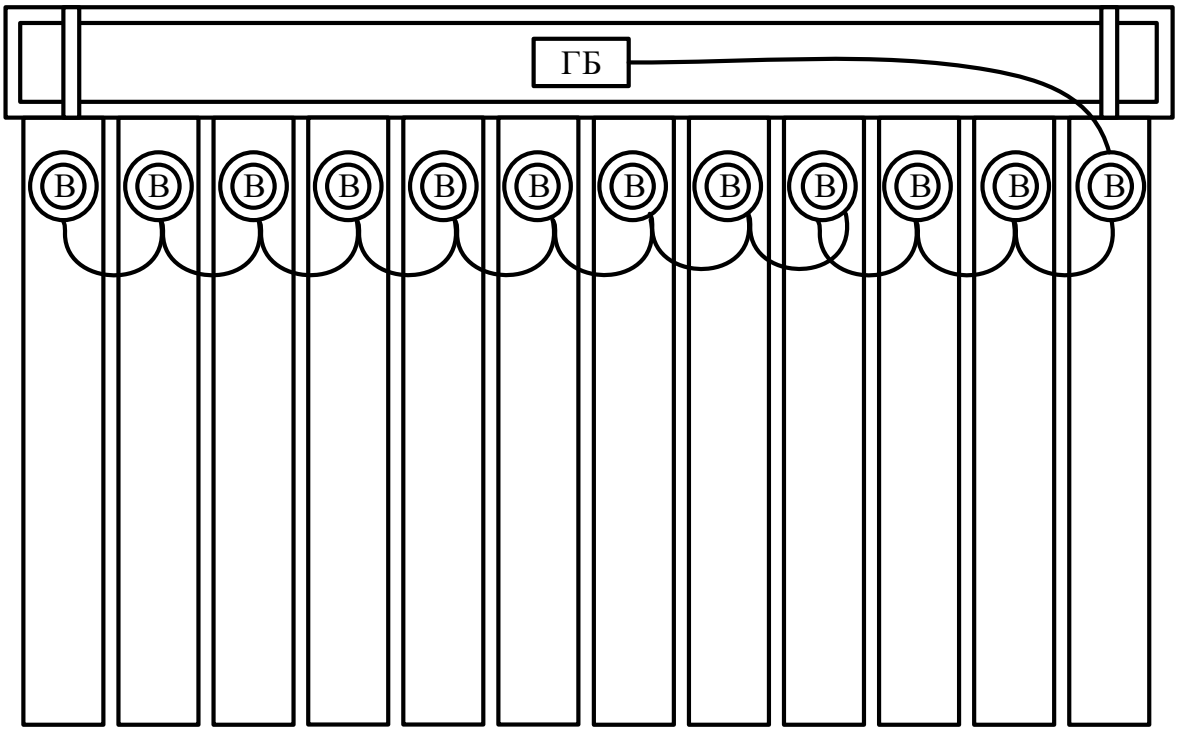


Рис. 2. Схема монтажа средств защиты информации на металлические жалюзи.

Плюсы:

1. Простота монтажа на стандартные элементы интерьера;
2. Простота эксплуатации;
3. Установка производится один раз. Далее средство защиты управляется через блок управления.

Минусы:

1. Не всегда подходят для нестандартных окон (размер, положение, наклон и т.п.);
2. Внешний вид. Виброизлучатели и соединительные провода никак не скрыты и не защищены от внешнего воздействия. Соответственно

конструкцию на жалюзи или рольставнях видно невооруженным взглядом;

3. Выход из строя. Так как конструкция средства защиты открыта и не защищена от внешнего воздействия, в процессе эксплуатации возможно непреднамеренное повреждение (обрыв проводов).

Второй вариант. Защитный экран, предназначенный для установки на стекло оконного проема на время проведения конфиденциальных переговоров. Изготовлен из полистирола, обычно белого цвета. Крепится к стеклу оконного проема с помощью магнитов и стоек. Схема монтажа защитного экрана на окно приведена на рис. 3.

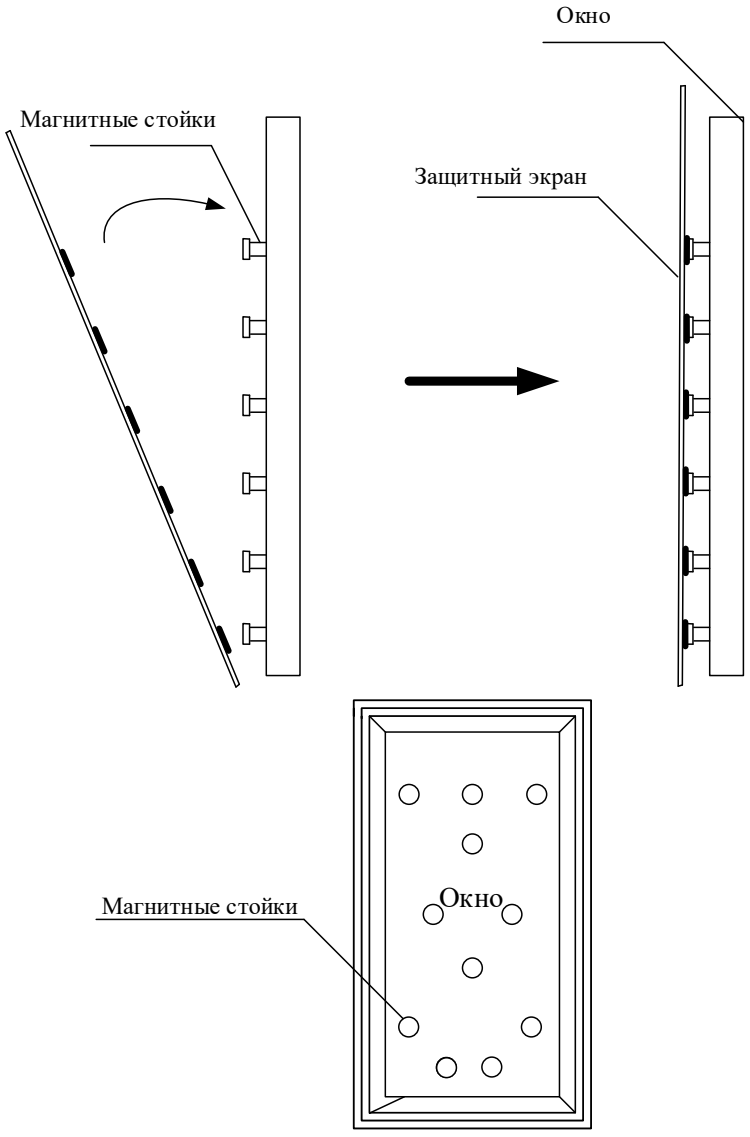


Рис. 3. Схема монтажа защитного экрана

Плюсы:

1. Стоимость. По сравнению с другими средствами защиты, является одним из самых выгодных;

2. Простота монтажа и эксплуатации. Для монтажа и эксплуатации данного средства защиты не требуется определенных знаний, связанных с электротехникой или настройкой средств защиты;
3. Изготавливается индивидуально по размерам заказчика. Может использоваться в помещениях с нестандартными оконными проемами;
4. За счет простоты исполнения шанс поломки при правильной эксплуатации практически отсутствует.

Минусы:

1. Необходимо устанавливать защитный экран каждый раз при проведении конфиденциальных переговоров, и снимать их после окончания;
2. В зависимости от размера защитного экрана для его установки может потребоваться несколько человек;
3. Когда защитный экран не используется, его нужно где-то хранить. Необходимо выделить место или отдельное помещение для хранения защитного экрана или экранов;
4. Магнитные стойки защитного экрана перманентно приклеиваются к стеклу оконного проема, влияя на внешний вид помещения. Также установленные экраны могут ухудшать внешний вид помещения.

Третий вариант. Внешние рольставни с электрическим приводом или ручной эксплуатацией. Устанавливаются на оконный проем снаружи помещения. Схема размещения внешних рольставен с электроприводом приведена на рис. 4.

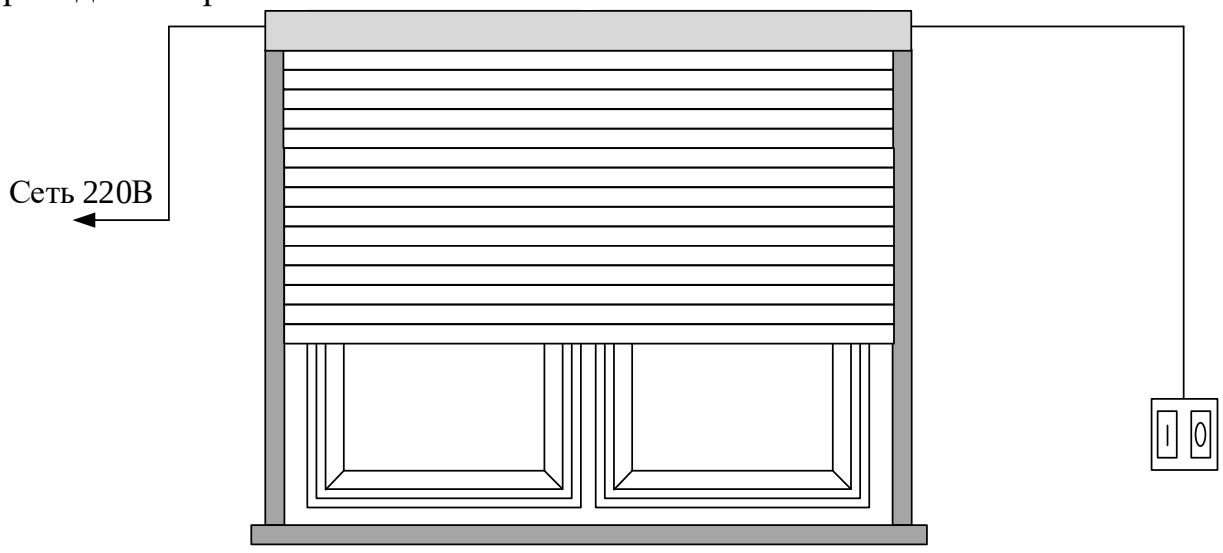


Рис. 4. Схема размещения внешних рольставен с электроприводом

Плюсы:

1. Стоимость. Зависит от размеров рольставен, исполнения (с приводом или без), и сложности установки, но в большинстве случаев находится на уровне защитных экранов;

2. Простота эксплуатации в случае исполнения с электроприводом, управление производится с помощью пульта управления;
3. Внешний вид. Относительно внутренней части помещения никак себя не выдает.

Минусы:

1. Если используется вариант без электропривода рольставни необходимо опускать и поднимать вручную;
2. При выходе из строя рольставен необходимо обращаться к специализированным ремонтным сервисам;
3. В зависимости от месторасположения здания или наличия у него исторической ценности установка внешних рольставен может быть запрещена;
4. Представляют собой видовой демаскирующий признак. Упрощает задачу злоумышленника найти помещение где обсуждается конфиденциальная информация.

Четвертый вариант. Смарт-пленка. Изготовлена с применением полимерного материала, способного при необходимости изменять свою прозрачность (светопропускаемость). Под действием напряжения жидкие кристаллы либо упорядочиваются и пропускают свет (становятся прозрачными), либо располагаются хаотично и свет не пропускают (непрозрачный вид). Схема работы смарт-пленки представлена на рис. 5.

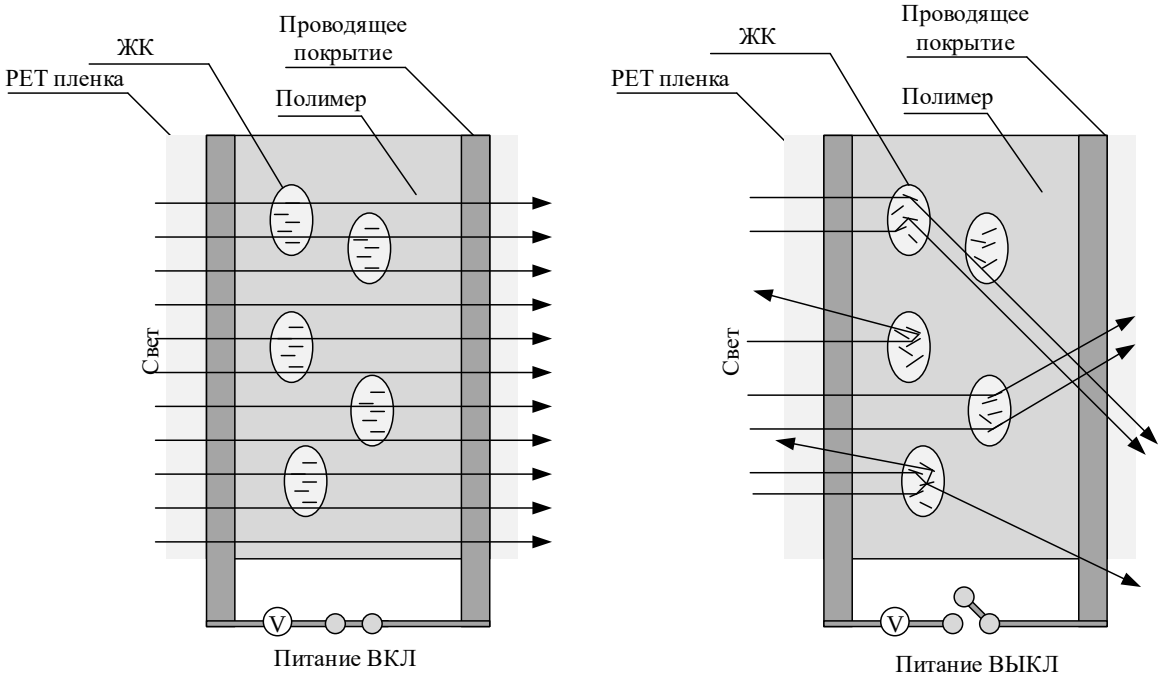


Рис. 5. Схема работы смарт-пленки

Плюсы:

1. Стоимость. При более сложном технологическом процессе изготовления, по стоимости сравнивается с защитными экранами;

2. Простота монтажа и эксплуатации. Монтаж осуществляется путем приклеивания пленки к стеклу оконного проема и подключения ее к источнику питания. Режим прозрачности управляется с помощью пульта управления;
3. Изготавливается индивидуально по размерам заказчика. Подходит для всех оконных проемов независимо от размера, положения, наклона;
4. Низкая вероятность поломки, за счет отсутствия большого количества составных частей;
5. В выключенном состоянии никак себя не выдает и не влияет на внешний вид помещения.

Минусы:

1. Зависимость от электросети. Для изменения прозрачности смарт-пленки необходимо напряжение. Так как данное решение энергоэффективно, то недостаток можно исправить подключенным источником бесперебойного питания;
2. В настоящее время не является сертифицированным средством защиты. Нет научно доказанных исследований, испытаний, подтверждающих эффективность данного решения для защиты информации от утечки по оптико-электронному каналу.

Лазерный микрофон

Лазерный микрофон позволяет осуществлять дистанционное прослушивание помещений по колебаниям оконного стекла. Данные колебания модулируют луч лазера, отражающийся от поверхности стекла и попадающий на фотоприемник для соответствующего преобразования и декодирования с помощью электронных устройств.

На рисунке приведены примеры схем ИК-передатчика и ИК-приемника.

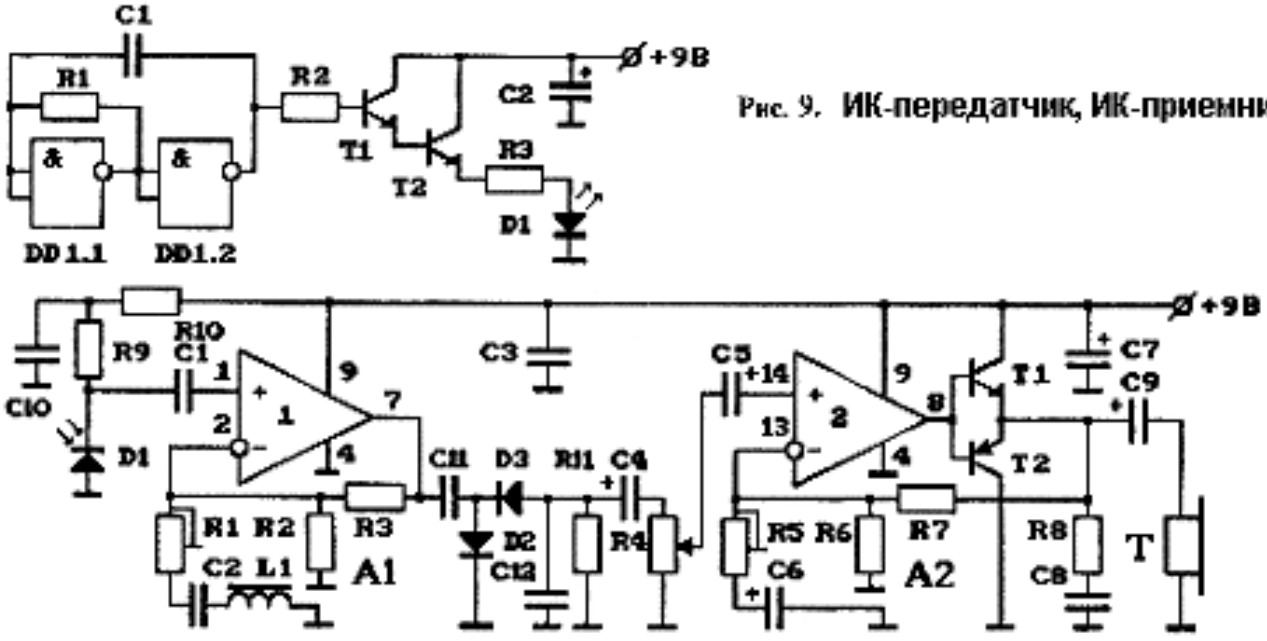


Рис. 9. ИК-передатчик, ИК-приемник

Данные устройства позволяют "считывать" акустическую информацию с оконного стекла, что позволяет, как и в случае лазерного микрофона, осуществлять дистанционное прослушивание помещений. Для этого сфокусированный луч ИК-передатчика направляется на оконное стекло. ИК-приемник принимает отраженный промодулированный сигнал демодулирует его, усиливает и воспроизводит.

Элементы для схемы ИК-передатчика:

R_1=50к-100к (R_1 и C_1 задают частоту генератора несущей - 30кГц-50кГц), R_2=1k, R_3=8-10 (задает ток через ИК-светодиод, среднее значение - 250мА-300мА); C_1=150, C_2=1000мкФ-4000мкФ; DD1 (DD1.1, DD1.2) - К561; D_1 - АЛ119А; T_1 - КТ3102, КТ315 или аналогичные транзисторы; T_2 - КТ815, КТ807 или аналогичные, возможно использование вместо T_1 и T_2 одного транзистора КТ827.

Элементы для схемы ИК-приемника:

R_1=100-500 (регулировка чувствительности ОУ1: К=1+R_3/R_1), R_2=200k-300k, R_3=300k-500k, R_4=30k-100k (регулировка громкости), R_5=1k-5k (регулировка чувствительности ОУ2: К=1+R_7/R_5), R_6=200k-300k, R_7=10k-50k, R_8=10, R_9=300k-500k, R_{10}=300k-500k, R_{11}=16k-24k (R_{11} и C_4 могут быть исключены из схемы, в этом случае R_4=16k-25k); C_1=0.1-0.2, C_3=0.1-0.3, C_4=0.3-5мкФ, C_5=1мкФ-10мкФ, C_6=5мкФ-20мкФ, C_7=50мкФ-500мкФ, C_8=0.1, C_9=100мкФ-500мкФ, C_{10}=0.1-0.2, C_{11}=0.3-1мкФ, C_{12}=9н-15н; L_1C_2 настраиваются на частоту 30-50 кГц, L_1 - 400-500 витков ПЭЛ 0.05-0.07 на каркасе от фильтра ПЧ радиоприемника. D1 - ФДК261 или аналогичные ИК-фотодиоды; D2,D3 - ГД507 или аналогичные (германевые - меньше порог); A1,A2 - ОУ ИС КР548УН1; T_1, T_2 - КТ3102, КТ3107 или КТ315, КТ361, или аналогичные комплементарные (парные) транзисторы; Т - ТМ-2А или аналогичные.

Литература

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – М.: Гостехкомиссия России, 2001.
2. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.
3. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия России, 1998.
4. Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. – М.: РЦИБ «Факел», 2008.

5. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 2000.
6. Glinsky A. Theremin: Ether Music and Espionage. – M: University of Illinois Press, Urbana, IL, 2000.
7. Wallace R., Melton H. K., Schlesinger H.R. Spycraft: The Secret History of the CIA’s Spytechs, from Communism to Al-Qaeda. – M.: Dutton/Penguin Group, New York, NY, 2008.
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие. – М.: ИТМО Санкт-Петербург, 2012 С. 112-115.
9. URL: http://www.npoanna.ru/Content.aspx?name=models.sonata-av4l
10. URL: https://nppgamma.ru/catalog/ustroystva_vibroakusticheskoy_zashchity/shorokh_5l/
11. URL: https://kamerton5.ru/
12. URL: https://pelena-256.ru/
13. URL: https://ru.wikipedia.org/wiki/Рольставни
14. URL: https://patents.google.com/patent/US5270843A/en

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Содержание основных научных понятий и категорий теории безопасности	**Подготовка докладов по темам:** Научные понятия и категорий теории безопасности.
2.	Угрозы информации. Информация как объект защиты	**Подготовка докладов по темам:** Информация как объект защиты.
3	Концептуальные документы в области защиты информации. Основные федеральные нормативные правовые акты. Основные подзаконные акты в области защиты информации	**Подготовка докладов по темам:** Концептуальные документы в области защиты информации.
4	Система государственных и отраслевых требований (стандартов) в области защиты информации. Особенности зарубежных стандартов защиты информации	**Подготовка докладов по темам:** Особенности зарубежных стандартов защиты информации.
5	ГОСТ Р ИСО/МЭК 15408-2002 – аутентичный вариант общих критериев	**Презентации по темам:** Система государственных и отраслевых требований в области защиты информации.

	безопасности информационных технологий	
6	Нормативные документы ФСТЭК России	**Подготовка докладов по темам:** Нормативные документы ФСТЭК России.
7	Общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Проведение сертификационных испытаний	**Презентации по темам:** Проведение сертификационных испытаний.
8	Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация на региональном и международном уровнях	**Презентации по темам:** Сертификация продукции, ввозимой из-за границы.
9	Общая характеристика. Концепция информационной безопасности предприятия и ее содержание. Политика информационной безопасности предприятия	**Подготовка докладов по темам:** Концепция Информационной безопасности предприятия и ее содержание.
10	Служба информационной безопасности предприятия	**Подготовка докладов по темам:** Служба информационной безопасности предприятия.

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, необходимой для освоения дисциплины (модуля)

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2.Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
4.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. —

Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
5. Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1.Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

11. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
12. http://informika.ru/ – образовательный портал.
13. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
14. www.biblioclub.ru - Универсальная библиотека онлайн.
15. www.rucont.ru - ЭБС «Руконт».
16. http://www.academy.it.ru/ – академия АЙТИ.
17. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
18. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
19. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

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

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 и др).