Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
Н.В. Бабина
«12» апреля 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.05.03 «ОЦЕНКА ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (ООО «НОВО», ООО «ЦБИ»)»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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: «Оценка защищенности конфиденциальной информации по техническим каналам от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)». – Королев МО: «Технологический университет», 2022.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.т.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

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

Целями изучения дисциплины является:

1. формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации от НСД;
2. усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации от НСД, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Основными **задачами** дисциплины являются:

1. Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации от НСД на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации;
2. Формирование у обучающихся правовой системы знаний, умений и навыков по защите информации от НСД;
3. Обеспечению информационной безопасности граждан, общества и государства, в частности раскрытие общих положений по защите информации от НСД;
4. Научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации от НСД;
5. ознакомить студентов с перспективными технологиями и методами защиты информации от НСД;
6. изучить современные методики применения и использования встроенных механизмов защиты информации от НСД;

7. научить студентов, порядку применения технических средств защиты информации от НСД.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

Необходимые умения:

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;
- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);

Трудовые действия:

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;
- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

2. Место дисциплины в структуре ОПОП

Дисциплина «Оценка защищенности конфиденциальной информации по техническим каналам от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очной формы составляет 2 зачетных единиц 72 часов.

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр 7	Семестр …	Семестр …
Общая трудоемкость	72	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	30	30			
Другие виды контактной работы	6	6			
Практическая подготовка	12	12			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Зачет	Зачет			

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

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час. очное	Занятия в интерактивной форме, час. очное	Практическая подготовка, час	Код компетенций
1	2	3	4		5

Тема 1. Правовые основы обеспечения защиты конфиденциальной информации. Государственная система защиты информации	3	3	2	2	ПК-1
Тема 2. Технические каналы утечки информации	3	3	2	2	ПК-1
Тема 3. Основы организации и обеспечения работ по технической защите конфиденциальной информации	3	3	2	2	ПК-3
Тема 4. Средства оценки защищенности информации от утечки по техническим каналам	3	3	3	2	ПК-4
Тема 5. Типовые средства защиты информации и особенности их эксплуатации	4	4	3	4	ПК-4
	16	162	120	**122**	

4.2. Содержание тем дисциплины

Тема 1. Правовые основы обеспечения защиты конфиденциальной информации
Государственная система защиты информации в Российской Федерации.
Законы Российской Федерации и другие нормативно-правовые документы, регламентирующие отношения субъектов в информационной сфере и деятельность организаций по технической защите конфиденциальной информации. Техническая защита конфиденциальной информации, обязанности и права субъектов информационных отношений. Лицензирование деятельности по технической защите конфиденциальной информации, сертификация средств защиты информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России.

Тема 2. Технические каналы утечки информации

Вводная часть. Особенности утечки информации. Возможные каналы утечки информации. Их краткая характеристика.
Каналы утечки речевой информации. Акустический и виброакустический каналы. Краткая характеристика речевой информации. Особенности распространения звуковых колебаний в различных средах. Примеры, механизмы реализации.
Утечка речевой информации по проводным коммуникациям. Акустоэлектрические преобразования и высокочастотное «навязывание» (облучение).
Каналы утечки информации возникающие при эксплуатации средств вычислительной техники. Побочные электромагнитные излучения и наводки (ПЭМИН). Физические основы возникновения каналов утечки информации за счет ПЭМИН. Структура каналов, особенности реализации. Примеры, механизмы реализации.
Физические основы функционирования канала утечки акустической информации, возникающего за счет прямого и модуляционного акустоэлектрических преобразований. Механизмы реализации. Электромагнитный, электродинамический, и др. эффекты. Примеры реализации.
Физические основы функционирования канала утечки акустической информации, возникающего за счет параметрических преобразований. Механизмы модуляции, в том числе параметрической.
Физические основы функционирования канала утечки акустической информации, возникающего за счет оптико-электронного (лазерного) излучения. Особенности выявления и защиты от съема информации по данному каналу.
Особенности утечки информации по техническим каналам с использованием закладочных устройств. Краткая характеристика возможных каналов утечки информации используемых закладочными устройствами. Структура и демаскирующие признаки закладочных устройств. Особенности их выявления и нейтрализации.
Основные критерии оценки защиты информации от утечки по техническим каналам.

Тема 2. Основы организации и обеспечения работ по технической защите конфиденциальной информации

Цели и задачи технической защиты конфиденциальной информации. Способы и средства их реализации. Классификация способов и средств технической защиты конфиденциальной информации. Основные механизмы защиты.
Подходы к созданию комплексной системы защиты конфиденциальной информации в организации. Определение перечня сведений конфиденциального характера, составляющих коммерческую тайну в организации. Общая последовательность и методика принятия управленческого решения на организацию защиты информации. Оценка обстановки. Выявление проблем. Постановка задачи на организацию технической защиты конфиденциальной информации. Определение путей и очередности решения вопросов технической защиты конфиденциальной информации. Разработка вариантов дальнейших действий. Моделирование, оценка эффективности и выбор оптимального варианта организационно-технических мер защиты. Формулирование управленческого решения. Разработка директивных указаний подчиненным.
Структура подразделений технической защиты информации. Основные принципы построения системы защиты конфиденциальной информации в организации. Функции и задачи подразделений технической защиты информации. Разработка концепции и политики информационной безопасности организации.
Аттестация объектов информатизации, как комплекс организационно-технических мероприятий, подтверждающий соответствие защищаемого объекта требованиям стандартов или иных нормативно-технических документов по безопасности информации. Планирование работ по технической защите конфиденциальной информации. Обоснование требований к системе защиты конфиденциальной информации. Требования к применяемым техническим средствам защиты информации.

Тема 4. Средства оценки защищенности конфиденциальной информации от утечки по техническим каналам

Методы оценки защищенности информации от утечки по техническим каналам. Модель канала утечки. Принципы оценки. Соотношение сигнал-шум. Методы достижения условий защищённости. Принципы проведения замеров и расчётов.

Обзор средств контроля защищенности. Состав контрольно-измерительной аппаратуры для проведения измерений уровней акустических (вибрационных) сигналов. Состав контрольно-измерительной аппаратуры для проведения измерений напряженности электромагнитного поля ПЭМИ от технических средств, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Состав контрольно-измерительной аппаратуры для проведения измерений напряжения, наведенного в токопроводящих коммуникациях информативного сигнала.

Тема 5. Типовые средства защиты конфиденциальной информации и особенности их эксплуатации

Общая характеристика средств защиты информации от утечки по техническим каналам. Их назначение, реализуемые функции, состав. Фильтры частотные. Ограничители малых сигналов. Генераторы шума. Принципы их работы. Конструктивные решения. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору средств защиты информации по видам объектов обрабатывающих конфиденциальную информацию: каналы связи, помещения для ведения конфиденциальных переговоров, автоматизированные системы и т.д. Рекомендации по установке, настройке и эксплуатации.

Обзор средств активной защиты: акустика, виброакустика, системы виброакустического зашумления, средства защиты слаботочных линий, постановщики помех сотовым телефонам, диктофонам.

Обзор средств выявления демаскирующих признаков закладочных устройств. Средства радиоконтроля, поисковая техника, средства неразрушающего контроля, досмотровая техника, средства дозиметрии. Изучение универсальных поисковых приборов, средств контроля проводных коммуникаций, средств активной защиты, подавителей диктофонов, сотовых телефонов, постановщиков помех.

Средства защиты от утечки по каналам ПЭМИН. Назначение. Обзор моделей. Технические характеристики, особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации. Генераторы шума. Диапазон. Размещение и выбор в зависимости от уровня опасного сигнала. Доработанные по специальным требованиям основные технические средства и системы. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.

Средства защиты сети питания. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Частотные фильтры. Особенности и принципы работы. Задерживающие и поглощающие. Построение системы электропитания и заземления. Линейное зашумление. Ограничители малых сигналов. Оценка эффективности. Линейные генераторы шума. Особенности применения. Оценка эффективности. Разнос, экранирование линий.

Устройства защиты телефонных линий. Назначение. Обзор моделей. Технические характеристики. Особенности применения. Рекомендации по выбору, установке, настройке и эксплуатации.

Рекомендации по проектированию, созданию и эксплуатации комплексных систем защиты конфиденциальной информации.

Организация и осуществление работ по выявлению технических каналов утечки информации, образованных при помощи закладочных устройств. Выявление демаскирующих признаков закладочных устройств при поиске.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Оценка защищенности конфиденциальной информации по техническим каналам от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)» приведена в Приложении 1.

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

Основная литература:

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3http://znanium.com/bookread2.php?book=549914

2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4http://znanium.com/bookread2.php?book=402686

Дополнительная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6http://znanium.com/bookread2.php?book=474838

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429070

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал;

2. **http://informika.ru/** – образовательный портал;

3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи;

4. **www.biblioclub.ru** - Универсальная библиотека онлайн;

5. **www.rucont.ru** - ЭБС «Руконт»;

6. **http://www.academy.it.ru/ –** академия АЙТИ;

7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации;

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

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

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

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

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

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

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

9. Методические указания для обучающихся, по освоению дисциплины

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).

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Оценка защищенности, конфиденциальной информации по техническим каналам от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)»

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.

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

«ОЦЕНКА ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (ООО «НОВО», ООО«ЦБИ»)»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1 -5	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Тема:1-5	- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию	- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;	- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
3	ПК-4	Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных	Тема 1-5	- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности	- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять	- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки

		ситуаций		применяемых программных, программно-аппаратных и технических средств защиты информации;	нарушения в области ИБ (ЗИ);	защищенности и регламенты обеспечения работоспособности систем ЗИ;

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-1,3,4	*Доклад*	*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*	*Например:* *Проводится в письменной и/или устной форме.* *Критерии оценки:* *1. Соответствие содержания доклада заявленной тематике (1 балл).* *2. Качество источников и их количество при подготовке работы (1 балл).* *3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).* *4. Качество самой представленной работы (1 балл).* *5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).* *Максимальная сумма баллов - 5 баллов.*
ПК-1,3,4	*Выполнение контрольной работы*	*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*	*При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида*

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

Примерная тематика докладов в презентационной форме:

1.Основы физической защиты информации на различных объектах, на средствах АСУ (ЭВТ) и в компьютерных сетях.
2. Основные источники угроз и характеристика объектов информационного воздействия.
3. Характеристика происхождения информационных угроз и атак, источники угроз, предпосылки их появления.
4. Виды атак информационным системам, основные нарушения целостности информации.
5. Характеристика каналов утечки информации.
6. Особенности электромагнитных каналов утечки информации.
7. Особенности акустических каналов утечки информации.
8. Классификация каналов несанкционированного получения информации и виды потерь.
9. Основные функции системы физической защиты (СФЗ) и их особенности.
10. Основные характеристики эффективной системы физической защиты и основные критерии проектирования СФЗ, их характеристика.
11. Архитектура систем защиты информации и методы оценки эффективности их применения.
12. Порядок построения систем защиты информации, ядро СФЗ.
13. Понятие ресурсов системы защиты информации.
14. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
15. Классификация внешних датчиков охранной сигнализации и их особенности применения.
16. Классификация внутренних датчиков охранной сигнализации и их особенности применения.
17. Сбор данных о тревоге и порядок их оценки.
18. Телевизионные системы оценки сигнала тревоги и их характеристика.
19. Характеристика систем освещения и их особенности.
20. Характеристика систем сбора данных о тревоге и их отображения (ССДО).
21. Характеристика сил реагирования и средств связи, порядок их применения.
22. Основные требования к безопасности информационных систем.
23. Классы защищённости средств вычислительной техники от несанкционированного доступа.
24. Методы и модель оценки уязвимости информации.
25. Особенности эмпирического подхода к оценке уязвимости информации.
26. Основные допущения в моделях оценки уязвимости информации.
27. Характеристика систем с полным перекрытием.

28. Рекомендации по использованию моделей оценки уязвимости информации.
29. Критерии оценки безопасности информационных технологий, стратегия защиты информации.
30. Организация требований к системам безопасности в рамках документа Общие критерии.
31. Способы и средства защиты информации, их классификация и особенности применения.
32. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
33. Характеристика семирубежной модели защиты информации.
34. Последовательность анализа и оценки проектирования систем физической защиты.
35. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
36. Основные инструменты для проведения количественного анализа СФЗ, характеристика компьютерных моделей.
37. Методы определения требований к физической защите информации.
38. Классификация требований к физической защите информации в зависимости от средств защиты.
39. Порядок обеспечения безопасности объектов с помощью средств физической защиты информации, последовательность решения задачи.
40. Особенности технических средств обеспечения физической безопасности подвижных объектов.
41. Характеристика основных средств охранной сигнализации для физических лиц.
42. Характеристика технических средств физической защиты.
43. Особенности механических систем физической защиты.
44. Характеристика систем оповещения.
45. Характеристика систем опознавания.
46. Характеристика оборонительных систем.
47. Оборудование центрального поста персонала охраны и комплекса физической защиты.
48. Характеристика средств контроля доступа на объекты.
49. Характеристика биометрических систем идентификации персонала.
50. Характеристика приборов для обнаружения контрабанды.
51. Характеристика и основные показатели охранной системы “МИККОМ AS 101”.
52. Характеристика и основные показатели системы “Урядник”.
53. Характеристика и основные показатели системы “Форпост”.

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

Формой контроля знаний по дисциплине «Защита информации от несанкционированного доступа» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1,3,4	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	ПК-1,3,4	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	Зачет	ПК-1,3,4	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** 1. знание лексического и грамматического материала;

образовательного процесса				Время, отведенное на процедуру – 15 минут.		2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях в течение семестра; 4. ответ на вопросы зачета. **«Не зачтено»:** 1. демонстрирует частичные знания по темам дисциплин; 2. незнание лексического и грамматического материала; 3. неумение использовать и применять полученные знания; 4. не работал на практических занятиях; 5. не отвечает на вопросы зачета.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1.Основы физической защиты информации на различных объектах, на средствах АСУ (ЭВТ) и в компьютерных сетях.
2. Основные источники угроз и характеристика объектов информационного воздействия.
3. Характеристика происхождения информационных угроз и атак, источники угроз, предпосылки их появления.
4. Виды атак информационным системам, основные нарушения целостности информации.
5. Характеристика каналов утечки информации.
6. Особенности электромагнитных каналов утечки информации.
7. Особенности акустических каналов утечки информации.

8. Классификация каналов несанкционированного получения информации и виды потерь.
9. Основные функции системы физической защиты (СФЗ) и их особенности.
10. Основные характеристики эффективной системы физической защиты и основные критерии проектирования СФЗ, их характеристика.
11. Архитектура систем защиты информации и методы оценки эффективности их применения.
12. Порядок построения систем защиты информации, ядро СФЗ.
13. Понятие ресурсов системы защиты информации.
14. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
15. Классификация внешних датчиков охранной сигнализации и их особенности применения.
16. Классификация внутренних датчиков охранной сигнализации и их особенности применения.
17. Сбор данных о тревоге и порядок их оценки.
18. Телевизионные системы оценки сигнала тревоги и их характеристика.
19. Характеристика систем освещения и их особенности.
20. Характеристика систем сбора данных о тревоге и их отображения (ССДО).
21. Характеристика сил реагирования и средств связи, порядок их применения.
22. Основные требования к безопасности информационных систем.
23. Классы защищённости средств вычислительной техники от несанкционированного доступа.
24. Методы и модель оценки уязвимости информации.
25. Особенности эмпирического подхода к оценке уязвимости информации.
26. Основные допущения в моделях оценки уязвимости информации.
27. Характеристика систем с полным перекрытием.
28. Рекомендации по использованию моделей оценки уязвимости информации.
29. Критерии оценки безопасности информационных технологий, стратегия защиты информации.
30. Организация требований к системам безопасности в рамках документа Общие критерии.
31. Способы и средства защиты информации, их классификация и особенности применения.
32. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
33. Характеристика семирубежной модели защиты информации.
34. Последовательность анализа и оценки проектирования систем физической защиты.
35. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
36. Основные инструменты для проведения количественного анализа СФЗ, характеристика компьютерных моделей.
37. Методы определения требований к физической защите информации.
38. Классификация требований к физической защите информации в зависимости от средств защиты.

39. Порядок обеспечения безопасности объектов с помощью средств физической защиты информации, последовательность решения задачи.
40. Особенности технических средств обеспечения физической безопасности подвижных объектов.
41. Характеристика основных средств охранной сигнализации для физических лиц.
42. Характеристика технических средств физической защиты.
43. Особенности механических систем физической защиты.
44. Характеристика систем оповещения.
45. Характеристика систем опознавания.
46. Характеристика оборонительных систем.
47. Оборудование центрального поста персонала охраны и комплекса физической защиты.
48. Характеристика средств контроля доступа на объекты.
49. Характеристика биометрических систем идентификации персонала.
50. Характеристика приборов для обнаружения контрабанды.
51. Характеристика и основные показатели охранной системы “МИККОМ AS 101”.
52. Характеристика и основные показатели системы “Урядник”.
53. Характеристика и основные показатели системы “Форпост”.

Тестовые задания для контроля остаточных знаний

Вариант № 1

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:
- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?
- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
- 2000
- 1967
- 1998

- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств,

подлежащих защите

Вариант № 2

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:
- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:
- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?
- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?
- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания

автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:
- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:
- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 3

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:
- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования

•ключным системам

4. Простейшим из шифров замены является:
•одноалфавитная подстановка
•многоалфавитная замена
•гомофонический шифр
•малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
•4
•3
•40
•7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
•любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
•формализованных и относительно стойких к ручному криптоанализу шифров
•криптосистем со строгим математическим обоснованием криптостойкости
•вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?
•с 1970-х гг.
•с 1980-х гг.
•с 1990-х гг.
•с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
•дейтаграммный
•виртуальный
•параллельный
•перпендикулярный

9. Сколько уровней в эталонной модели OSI?
•1
•13
•10
•7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?
- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:
- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:
- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи

•введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

4.2.Типовые вопросы, выносимые на зачет

Основы физической защиты информации на различных объектах, на средствах АСУ (ЭВТ) и в компьютерных сетях.
2. Основные источники угроз и характеристика объектов информационного воздействия.
3. Характеристика происхождения информационных угроз и атак, источники угроз, предпосылки их появления.
4. Виды атак информационным системам, основные нарушения целостности информации.
5. Характеристика каналов утечки информации.
6. Особенности электромагнитных каналов утечки информации.
7. Особенности акустических каналов утечки информации.
8. Классификация каналов несанкционированного получения информации и виды потерь.
9. Основные функции системы физической защиты (СФЗ) и их особенности.
10. Основные характеристики эффективной системы физической защиты и основные критерии проектирования СФЗ, их характеристика.
11. Архитектура систем защиты информации и методы оценки эффективности их применения.
12. Порядок построения систем защиты информации, ядро СФЗ.
13. Понятие ресурсов системы защиты информации.
14. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
15. Классификация внешних датчиков охранной сигнализации и их особенности применения.
16. Классификация внутренних датчиков охранной сигнализации и их особенности применения.
17. Сбор данных о тревоге и порядок их оценки.
18. Телевизионные системы оценки сигнала тревоги и их характеристика.
19. Характеристика систем освещения и их особенности.
20. Характеристика систем сбора данных о тревоге и их отображения (ССДО).
21. Характеристика сил реагирования и средств связи, порядок их применения.
22. Основные требования к безопасности информационных систем.
23. Классы защищённости средств вычислительной техники от несанкционированного доступа.
24. Методы и модель оценки уязвимости информации.
25. Особенности эмпирического подхода к оценке уязвимости информации.
26. Основные допущения в моделях оценки уязвимости информации.
27. Характеристика систем с полным перекрытием.
28. Рекомендации по использованию моделей оценки уязвимости информации.
29. Критерии оценки безопасности информационных технологий, стратегия защиты информации.

30. Организация требований к системам безопасности в рамках документа Общие критерии.
31. Способы и средства защиты информации, их классификация и особенности применения.
32. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
33. Характеристика семирубежной модели защиты информации.
34. Последовательность анализа и оценки проектирования систем физической защиты.
35. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
36. Основные инструменты для проведения количественного анализа СФЗ, характеристика компьютерных моделей.
37. Методы определения требований к физической защите информации.
38. Классификация требований к физической защите информации в зависимости от средств защиты.
39. Порядок обеспечения безопасности объектов с помощью средств физической защиты информации, последовательность решения задачи.
40. Особенности технических средств обеспечения физической безопасности подвижных объектов.
41. Характеристика основных средств охранной сигнализации для физических лиц.
42. Характеристика технических средств физической защиты.
43. Особенности механических систем физической защиты.
44. Характеристика систем оповещения.
45. Характеристика систем опознавания.
46. Характеристика оборонительных систем.
47. Оборудование центрального поста персонала охраны и комплекса физической защиты.
48. Характеристика средств контроля доступа на объекты.
49. Характеристика биометрических систем идентификации персонала.
50. Характеристика приборов для обнаружения контрабанды.
51. Характеристика и основные показатели охранной системы “МИККОМ AS 101”.
52. Характеристика и основные показатели системы “Урядник”.
53. Характеристика и основные показатели системы “Форпост”.

**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.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

«ОЦЕНКА ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (ООО «НОВО»,ООО «ЦБИ»)»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является:

1. формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации от НСД;
2. усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации от НСД, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

Задачами дисциплины являются:

1. Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации от НСД на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации;
2. Формирование у обучающихся правовой системы знаний, умений и навыков по защите информации от НСД;
3. Обеспечению информационной безопасности граждан, общества и государства, в частности раскрытие общих положений по защите информации от НСД;
4. Научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации от НСД;
5. Ознакомить студентов с перспективными технологиями и методами защиты информации от НСД;
6. Изучить современные методики применения и использования встроенных механизмов защиты информации от НСД;
7. Научить студентов, порядку применения технических средств защиты информации от НСД.

2. Указания по проведению практических занятий

Тема 1. Технология контроля санкционированных событий. Парольная аутентификация

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.
2. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).
3. Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Продолжительность занятия:8 часов

Тема 2. Аутентификация с помощью биометрических характеристик

Практическое занятие 2.

Вид практического занятия**: *подготовка доклада.***

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код

аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

2. Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

3. Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамаля. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

4. Свойства хэш-функци. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHS, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Продолжительность занятия:8 часов

3. Указания по проведению лабораторных работ

(учебным планом не предусмотрено)

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

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

Учебные вопросы

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:
   - просмотреть предварительно созданный с помощью редактора свой текстовый файл;
   - выполнить для этого файла шифрование;
   - просмотреть в редакторе зашифрованный файл;

- просмотреть гистограммы исходного и зашифрованного текстов;
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование
- расшифровать зашифрованный текст:
  - с помощью программы, после чего проверить в редакторе правильность расшифрования.
  - вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

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

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

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

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

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

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

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

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

Продолжительность занятия: часов

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

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

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

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

Учебные вопросы

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

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

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

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

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

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

Продолжительность занятия: часов

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

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

Учебные вопросы

1. Проверить на простоту два произвольных целых числа разрядностью не менее 5.
2. Распределение простых чисел.

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

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

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

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

3. Методы генерации простых чисел.

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

Расчет производится для всех $k <= 10$.

3.2.Для интервала (1500, 1500 + 300):

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

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

удовлетворяющих этому тесту;
в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основания ми в тесте Ферма. Вычислить количество *P2* вероятно простых чисел, удовлетворяющих этому тесту. Проанализировать полученные данные.
3.3. Известно, что в заданном интервале имеются числа Кармайкла. Найти их.
Варианты интервалов:
(1050, 1050 + 100);
(1700, 1700+ 100);
(2400, 2400 + 100).
4. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта.

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

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

Продолжительность занятия: часов

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

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

Учебные вопросы

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой, изложенными выше. Запустить программу labWork6.exe, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.
2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.
3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.
4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.

5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.
6. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта

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

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

Продолжительность занятия: часов

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 2. Технические каналы утечки информации**	***Подготовка докладов по темам:*** 1. Какие свойства информации, влияющие на ее безопасность, вы знаете? 2. Определите виды, источники и носители защищаемой информации. 3. Основные направления инженерно-технической защиты информации. 4. Какие основные характеристики технических каналов утечки информации вы знаете? 5. Структура, классификация и основные характеристики технических каналов утечки ин- формации. 6. Перечислите принципы защиты информации техническими средствами. 7. Что такое модель и моделирование?
2.	**Тема 3. Основы организации и обеспечения работ по технической защите конфиденциальной информации**	***Подготовка докладов по темам:*** 8.Что такое аналитическая модель системы? 9. Моделирование случайных величин и их законы распределения. 10. Какие числовые характеристики случайных величин вы знаете? 11. Что описывает нижеприведенная формула? Поясните основные ее параметры.

		12. Какие статистические оценки знаете? Как определить их точность? 13. Аппроксимация результатов статистического моделирования. 14. Что такое адекватная модель?
3	**Тема 4. Средства оценки защищенности информации от утечки по техническим каналам**	***Подготовка докладов по темам:*** 15. Принципы моделирования объектов защиты. 16. Моделирование угроз безопасности информации. 17. Методические рекомендации по выбору рациональных вариантов защиты. 18. Основные понятия теории случайных процессов. 19. Классификация и основные характеристики случайных процессов. 20. Дайте определение марковских процессов. 21. Перечислите задачи защиты информации ТКС в условиях конфликта.
4	**Тема 5. Типовые средства защиты информации и особенности их эксплуатации**	***Подготовка докладов по темам:*** 22.. Понятие конфликта. Способы разрешения конфликта в ТКС. 23. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. 24. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия. 25. Какие виды контроля эффективности инженерно-технической защиты информации вы знаете? 26. Какие предъявляются требования по защите информации от утечки по техническим каналам? 27. Дайте классификацию методов и средств защиты информации от технических разведок. 28. Математическая модель канала утечки информации применительно к техническим разведкам.

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).

5.4.Примерная тематика контрольных работ:

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.

2. Представление сил и средств защиты информации в виде системы.

3. Структура, классификация и основные характеристики технических каналов утечки ин-формации. Простые и составные технические каналы утечки информации.

4. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.

5. Распространение оптических сигналов в атмосфере и в светопроводах.

6. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.

7. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.

8. Принципы защиты информации техническими средствами.

9. Основные направления инженерно-технической защиты информации.

10. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации.

11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

12. Основные теоремы теории вероятностей.

13. Моделирование случайных величин и их законы распределения.

14. Статистические оценки и их точность.

15. Аппроксимация результатов статистического моделирования.

16. Основные понятия теории случайных процессов, их классификация и основные характери-стики.

17. Марковские процессы с дискретными состояниями.

18. Марковские процессы с дискретными состояниями и непрерывным временем.

19. Стационарные случайные процессы.

20. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.

21. Принципы моделирования объектов защиты.

22. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.

23. Задачи защиты информации ТКС в условиях конфликта.

24. Понятие конфликта. Способы разрешения конфликта в ТКС.

25. Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия.

26. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.

27. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

28. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.

29. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.

30. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.

31. Способы оценки безопасности речевой информации в помещении.

32. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.

33. Способы оценки размеров зон I и II.

34. Основные задачи, структура и характеристика государственной системы противодействия технической защите.

Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

36. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.

37. Принципы действия аппаратуры технических разведок.

38. Классификация методов и средств защиты информации от технических разведок.

39. Классификация методов инженерно-технической защиты информации.

40. Инженерная защита и техническая охрана объектов.

41. Пространственное, энергетическое и структурное скрытие информации и ее носителей.

42. Дезинформирование, как метод скрытия.

43. Математическая модель канала утечки информации применительно к техническим разведкам.

44. Пространственное скрытие объектов наблюдения и сигналов.

45. Структурное и энергетическое скрытие объектов наблюдения.

46. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.

47. Энергетическое скрытие радио и электрических сигналов.

48. Классификация методов инженерной защиты и технической охраны объектов защиты.

49. Инженерные конструкции. Автономные и централизованные системы охраны

50. Модели злоумышленника.

51. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации уг-роз и управления.

52. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.

53. Комплекс технических средств охраны.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3http://znanium.com/bookread2.php?book=549914

2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4http://znanium.com/bookread2.php?book=402686

Дополнительная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6http://znanium.com/bookread2.php?book=474838

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429070

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru/** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности

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

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

Электронные ресурсы образовательной среды Университета

Информационно-справочные системы (Консультант+; Гарант).

Рабочая программа и методическое обеспечение по курсу «Оценка защищенности, конфиденциальной информации по техническим каналам от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)»