



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

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

« » 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.02.03. «ОСНОВЫ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ

СПЕЦИАЛЬНЫХ РАБОТ

ПО ВЫЯВЛЕНИЮ ЗАКЛАДОЧНЫХ УСТРОЙСТВ

(ООО «НОВО», НТЦ «ЗАРЯ») »

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

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

Автор: Панцыр Р.Я. Рабочая программа дисциплины (модуля): Основы организации и обеспечения специальных работ по выявлению закладочных устройств.(ООО «НОВО», НТЦ «ЗАРЯ»). – Королев МО: «Технологический Университет», 2023

Рецензент: Журавлев С.И.

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.Е. к.в.и. доцент			
Год утверждения (переподтверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023г.			

Рабочая программа согласована:

Руководитель ОПОП ВО



Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

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

2

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

Целью изучения дисциплины является формирование у слушателей специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества и методики постановки задач концептуального проектирования систем информационной безопасности региона, приобретение навыков в применении современных технологий при проектировании информационной безопасности объектов регионального уровня.

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

следующие компетенции:

Профессиональные компетенции:

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

- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности).

Основными задачами дисциплины являются:

- ознакомление слушателей с методологическими подходами постановки задач при проектировании систем информационной безопасности региона, а также с основными методами определения параметров, характеристик и структуры системы информационной безопасности;

- формирование у слушателей способности самостоятельно решать поставленные задачи в области проектирования систем информационной безопасности с помощью современных принципов, методов, сил и средств в различных организационных структурах региона, по базовым направлениям и применительно к типовым информационным объектам.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

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

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

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

Необходимые знания:

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии

организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

- 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 «Основы организации и обеспечения специальных работ по выявлению закладных устройств» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01. «Информационная безопасность».

Дисциплина «Основы организации и обеспечения специальных работ по выявлению закладных устройств» базируется на ранее изученных в бакалавриате дисциплинах «Основы исследований информационной безопасности», «Основы информационной безопасности», на одновременно изучаемых дисциплинах: «Защищенные информационные системы» и компетенциях: УК-1; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины «Теоретические основы компьютерной безопасности» являются базовыми для изучения последующих дисциплин «Информационно-аналитические системы безопасности», «Информационная безопасность финансово-кредитных структур», «Компьютерное моделирование информационных процессов и технологий» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации)

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетные единицы, 216 часов.

Таблица 1

Виды занятий	Всего часов	Семестр первый	Семестр ...	Семестр ...	Семестр ...
Общая трудоемкость	216	216			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	70	70			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	32	32			
Другие виды контактной работы*	6	6			
Лабораторные работы (ЛР)					
Практическая подготовка	нет	нет			
Самостоятельная работа	144	144			
<i>Курсовые работы (проекты) *</i>					
<i>Расчетно-графические работы*</i>					
<i>Контрольная работа *</i>					
<i>Текущий контроль знаний *</i>	Тест	Тест			
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. очн/заоч	Практические занятия, час очн/заоч	Занятия в интерактивной форме, час очн/заоч	Код компетенций
Тема 1. Технические каналы утечки информации.	8	8	4	ПК-3
Тема 2. Способы и средства защиты информации от утечки по техническим каналам.	8	8	4	ПК-2
Тема 3. Методы и средства контроля эффективности технической ЗИ	8	8	4	ПК-2,3
Тема 4. Организация технической защиты информации	8	8	4	ПК-2,3
Итого:	32	32	16	

4.2. Содержание тем дисциплины

Тема 1. Технические каналы утечки информации

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы.

Самостоятельное изучение. Основные параметры системы защиты информации.

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.

Самостоятельное изучение. Характеристика и возможности оптических, акустических радиоэлектронных и материально-вещественных каналов утечки информации.

Распространение сигналов в технических каналах утечки информации
Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.
Распространение оптических сигналов в атмосфере и в светопроводах.
Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.

Самостоятельное изучение. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.

Тема 2. Способы и средства защиты информации от утечки по техническим каналам

Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.

Самостоятельное изучение. Показатели эффективности инженерно-технической защиты информации.

Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

Самостоятельное изучение. Понятие о текущей и эталонной признаковой модели.

Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования.

Самостоятельное изучение. Оценка качества статистической модели.

Основные понятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями. Марковские процессы с дискретными состояниями и непрерывным временем. Стационарные случайные процессы.

Самостоятельное изучение. Основные положения теории нестационарных моментов марковских сетей.

Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.

Самостоятельное изучение Способы оптимизации мер инженерно-технической защиты информации.

Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС.

Самостоятельное изучение. Основные понятия рефлексивных игр.

Информационный конфликт (виды, варианты реализации). Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

Самостоятельное изучение. Разрешение конфликта в условиях рефлексивных игр. Разработка матрицы конфликтного взаимодействия для типовых ТКС.

Тема 3. Методы и средства контроля эффективности технической ЗИ

Контроль эффективности инженерно-технической защиты информации.

Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.

Самостоятельное изучение. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Показатели эффективности функционирования средств защиты информации в ТКС.

Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения. Способы оценки безопасности речевой информации в помещении. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств. Способы оценки размеров зон I и II.

Самостоятельное изучение. Оценка дальности перехвата сигналов.

Методика оценки эффективности ТКС в различных условиях функционирования.

Тема 4. Организация технической защиты информации

Государственная система защиты информации. 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.

Самостоятельное изучение. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.

Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок.

Самостоятельное изучение. Методический подход к оценке эффективности защиты информации от технических разведок.

Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственное, энергетическое и структурное скрывание информации и ее носителей. Дезинформирование, как метод скрывания. *Самостоятельное изучение* Комплексное применение методов защиты.

Математическая модель канала утечки информации применительно к техническим разведкам.

Самостоятельное изучение. Математическая модель канала акустической утечки информации.

Методы скрывания информации и ее носителей Пространственное скрывание объектов наблюдения и сигналов. Структурное и энергетическое скрывание объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрывание радио и электрических сигналов.

Самостоятельное изучение. Виды и условия зашумления.

Методы инженерной защиты и технической охраны объектов.

Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Комплекс технических средств охраны.

Самостоятельное изучение Автоматизация процессов охраны.

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 «Основы организации и

обеспечения специальных работ по выявлению закладочных устройств (ОАО «НОВО»)» приведена в Приложении 1.

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

Основная литература:

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/237770> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2. Алёшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алёшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167600> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3. Система охраны государственной тайны : учебное пособие / составители Е. З. Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 138 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/261902> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

4. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. — Новосибирск : СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/222380> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. <http://www.academy.it.ru/> – академия АЙТИ.

9. Методические указания для обучающихся, по освоению дисциплины

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

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

- **Перечень программного обеспечения:** MSOffice, PowerPoint.
- **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.

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

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

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**ОСНОВЫ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ СПЕЦИАЛЬНЫХ
РАБОТ ПО ВЫЯВЛЕНИЮ ЗАКЛАДОЧНЫХ УСТРОЙСТВ
(ООО «НОВО», НТЦ «ЗАРЯ»)**

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции), обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.	Тема: 1,2,3,4	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	ПК-2.2. проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.
2.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности)	Тема: 1,2,3,4.	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

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

			<p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-2,3	Контрольная работа	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком уровне</u>) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> • <i>компетенция освоена на <u>продвинутом уровне</u> – 4 балла;</i> • <i>компетенция освоена на <u>базовом уровне</u> – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p>	<p>Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>

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. 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 информации.
6. Перечислите принципы защиты информации техническими средствами.
7. Что такое модель и моделирование?
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?
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.
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.

Примерная тематика заданий на контрольную работу:

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 информации. 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, выделяемые 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 характеристики.
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 скрывание информации и ее носителей.
42. Дезинформирование, как метод скрывания.
43. Математическая модель канала утечки информации применительно к техническим разведкам.
44. Пространственное скрывание объектов наблюдения и сигналов.
45. Структурное и энергетическое скрывание объектов наблюдения.
46. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.
47. Энергетическое скрывание 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 угроз и управления.
52. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.
53. Комплекс технических средств охраны.

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

Формой контроля знаний по дисциплине «Основы организации и обеспечения специальных работ по выявлению закладочных устройств» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающих знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ПК-2 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%
Согласно учебному плану	тестирование	ПК-2 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%

Согласно учебному плану	Экзамен	ПК-2 ПК-3	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	<p>Критерии оценки:</p> <p>«Отлично»:</p> <ol style="list-style-type: none"> 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. <p>«Хорошо»:</p> <ul style="list-style-type: none"> • 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 <p>«Удовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание неумение
-------------------------	---------	--------------	-----------	--	---	---

					использовать и применять полученные знания на практике; • не работал на практических занятиях; «Неудовлетвор и-тельно»: • демонстрир ирует 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.

4.1. Типовые вопросы, выносимые на тестирование

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

1-е тестирование:

1. Что понимается под информационной угрозой?

- совокупность источников информации, условий, событий, среды и действий персонала, возникающая вследствие нарушения установленных ограничений в сфере производства, обращения и хранения информации;
- получение в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой информации;
- разрушающее информационное воздействие на систему, стремящееся нарушить требуемую функциональную взаимосвязь между входной и выходной информацией;
- это потенциальная возможность возникновения такой ситуации или события, следствием которой может стать нарушение безопасности информации.

2. По характеру проявления угрозы информации подразделяются на:

- внутренние;
- внешние;
- случайные;
- преднамеренные.

3. Выберите мероприятия, к которым сводится задача оценки угроз безопасности информации?

- обоснование структуры и содержания системы показателей, необходимых для исследований;
- обоснование структуры и содержания тех параметров, которые оказывают существенное влияние на значение показателей уязвимости информации;
- формирование структуры требований по безопасности информационных систем, которые обрабатывают информацию, содержащую государственную тайну;
- разработка комплексов моделей, отображающих функциональные зависимости показателей от параметров уязвимости информации во всех условиях жизнедеятельности объектов;
- разработка моделей для оценки показателей уязвимости при исследовании и практическом решении различных вопросов защиты;
- разработка комплекса мероприятий и процедур для совершенствования деятельности существующих систем защиты информации и объектов.

4. Относится ли несанкционированный доступ к защищённой информации к одному из видов информационных атак?

- да;
- нет.

5. На какие категории делятся компьютерные взломщики?

- бумеры;
- хакеры;

- кракеры;
- ламеры.

6. Что понимается под каналом утечки информации?

- совокупность источников и получателей информации, объединяющая такие средства, события, среду и действия персонала, возникающие вследствие нарушения установленных ограничений в сфере обращения информации и создающие потенциальную возможность утраты защищённых сведений, при которой они стали достоянием посторонних лиц;

- совокупность размещённых на ограниченной территории аппаратно-программных средств, функционирующих для организации совместного доступа и распределённой обработки информации в соответствии с принятой системой протоколов;

- пассивный компонент системы, хранящий, принимающий или передающий конфиденциальную информацию;

- возможность возникновения действий, направленных на нарушение конфиденциальности, целостности или доступности информации, а также на нелегальное использование других ресурсов посторонними лицами.

7. Индукционные каналы относят к техническим каналам утечки информации?

- да;
- нет.

8. Физические каналы относят к техническим каналам утечки информации?

- да;
- нет.

9. Гальванические каналы относят к техническим каналам утечки информации?

- да;
- нет.

10. Параметрические каналы относят к техническим каналам утечки информации?

- да;
- нет.

11. Выберите параметры, от которых зависит напряжение на проводе в цепи перехвата информации:

- сила тока;
- напряжение в сигнальном проводе;
- ёмкость между проводами;
- ёмкость между проводом и заземлённой подложкой.

12. Какие типы заземления устройств применяют?

- рабочее;
- защитное;
- технологическое;
- резервное.

13. Согласно требованиям длина заземляющих проводов для системы внутреннего телевидения не должна превышать:

- 5 м;
- 10 м;
- 50 м;
- 100 м.

14. Величина сопротивления заземления для предотвращения перехвата сигнала не должна превышать:

- 1 Ом;
- 4 Ом;
- 5 Ом;
- 10 Ом.

15. На какие виды делятся акустические каналы утечки информации?

- параметрические;
- вибрационные;
- оптико-электронные;
- гравитационные.

16. Что такое радиостетоскоп?

- прибор для демодуляции оптического луча лазера;
- закладное устройство для перехвата виброакустических сигналов;
- устройство для считывания голографических изображений;
- прибор для нанесения кодированной информации на персональные идентификационные карточки.

17. Выберите основные принципы для проектирования системы физической защиты:

- обнаружение нарушителя должно производиться на возможно большем расстоянии от цели нападения, а элементы задержки должны быть максимально приближены к ней;
- достаточность средств для обеспечения заданного уровня защиты;
- наличие тесной взаимосвязи между обнаружением нарушителя и оценкой ситуации оператором охраны;
- организация надёжной связи центрального поста охраны с силами реагирования.

18. Что понимается под системой физической защиты объектов?

- совокупность компонентов по противодействию несанкционированному получению конфиденциальной информации из защищаемых источников;
- организованная совокупность элементов (людей, процедур и технических средств), предназначенных для достижения поставленных целей по защите охраняемых объектов от нападения и проявления угроз;
- множество защитных элементов, обладающее некими новыми свойствами по сравнению с их отдельными составляющими и с относительно устойчивой схемой взаимосвязи между ними;
- организационно упорядоченный комплекс технических средств, технологий и носителей информации, реализующих информационные процессы для удовлетворения информационных потребностей пользователей и их защиты.

19. Выберите первичные функции системы физической защиты:

- интеграция людей, процедур и технических средств;
- обнаружение нарушителя;
- задержка нарушителя;
- реагирование охраны на нештатные ситуации.

20. Выберите основные показатели эффективности для функции обнаружения нарушителя:

- вероятность обнаружения действий нарушителя;
- время доведения сигнала тревоги;
- время, необходимое для получения и оценки сигнала тревоги;
- частота ложных тревог.

21. От чего зависит классификация ложных тревог по их источнику?

- от естественных условий;
- от вероятностных факторов;
- от инфраструктурных условий;
- от техногенных факторов.

22. Что является основным показателем эффективности для функции задержки нарушителя?

- вероятность обнаружения нарушителя;
- время на обнаружение препятствий;
- время, необходимое нарушителю для того, чтобы обойти каждое препятствие;
- средняя скорость продвижения нарушителя к охраняемому объекту.

23. Выберите основные типы реагирования для воспрепятствования успеху действий нарушителя:

- прерывание;
- нейтрализация;
- обнаружение;

- развёртывание.

24. Выберите основные показатели эффективности для сил реагирования:

- время между получением сообщения о действиях нарушителя и прерыванием этих действий;
- вероятность обнаружения нарушителя;
- вероятность доведения до сил реагирования сообщения о нарушителе;
- вероятность и время развёртывания сил реагирования;

25. Выберите основные характеристики эффективной системы физической защиты объектов:

- надёжность эшелонированной защиты;
- минимальные последствия отказов компонентов;
- избирательность действий компонентов защиты;
- сбалансированность элементов защиты.

26. Выберите приемлемые критерии эффективности при проектировании системы физической защиты:

- соотношение количества необходимых элементов и процедур системы физической защиты к их стоимости;
- выбор элементов и процедур в соответствии с их вкладом в суммарную эффективность системы физической защиты;
- выбор необходимых элементов и процедур в соответствии с требованием их наличия в системе;
- обеспечение баланса выбранных средств и процедур физической защиты с другими факторами аварийной безопасности, прочности конструкции и стоимости.

27. Выберите основные показатели эффективности для датчиков охранной сигнализации:

- время передачи сигнала;
- вероятность обнаружения нарушителя;
- частота ложных тревог;
- уязвимость по отношению к преодолению.

28. Зависит ли вероятность обнаружения датчика от условий его установки?

- да;
- нет.

29. Зависит ли вероятность обнаружения датчика от типа защищаемого объекта?

- да;
- нет.

30. Зависит ли вероятность обнаружения датчика от настройки его чувствительности?

- да;
- нет.

31. Выберите приемлемые способы преодоления системы датчиков:

- обход;
- дезинформация;
- обман;
- провокация.

32. Выберите приемлемые способы классификации внешних датчиков охранной сигнализации:

- пассивные или активные;
- скрытые или видимые;
- автономные или комплексные;
- действующие в пределах или вне пределов прямой видимости;

33. Датчики магнитного поля относятся к подземным внешним датчикам?

- да;
- нет.

34. Волоконно-оптический кабель относят к подземным внешним датчикам?

- да;
- нет.

35. Датчики электрического поля относят к подземным внешним датчикам?

- да;
- нет.

36. Чувствительность сейсмических датчиков зависит от грунта, в который их помещают?

- да;
- нет.

37. Сколько кабелей используют для прокладки коаксиального кабеля с отверстиями?

- один;
- два;
- четыре;
- не ограничено.

38. Ёмкостные датчики относят к датчикам, связанным с ограждением?

- да;
- нет.

39. Выберите устройства, которые используют в качестве чувствительных элементов на ограждениях:

- сейсмоприёмники;
- пьезоэлектрические датчики;
- микроволновые элементы;
- электромеханические датчики.

40. Какое минимальное усилие нужно приложить к чувствительному ограждению, чтобы вызвать сигнал тревоги?

- усилие порядка 1 кг;
- усилие порядка 5 кг;
- усилие порядка 11 кг;
- усилие порядка 15 кг.

41. Датчики электрического поля относят к индивидуально устанавливаемым внешним датчикам?

- да;
- нет.

42. Однопозиционные микроволновые датчики относят к индивидуально устанавливаемым внешним датчикам?

- да;
- нет.

43. На какой длине волны работают активные инфракрасные датчики?

- 0,1 мкм;
- 0,5 мкм;
- 0,9 мкм;
- 1,5 мкм.

44. Выберите приемлемые размеры зоны обнаружения для активного многолучевого инфракрасного датчика:

- 1м. на 1м.;
- 50см. на 2м.;
- 20см. на 1,5м.;
- 5см. на 1,8м.

45. Какой мощности эквивалентна излучаемая человеком тепловая энергия?

- 1 Вт;
- 10 Вт;
- 50 Вт;
- 100 Вт.

46. На каких частотах работают двухпозиционные СВЧ-датчики?

- 1 или 5 ГГц;

- 10 или 24 ГГц;
- 15 или 25 ГГц;
- 20 или 50 ГГц.

47. На каком максимальном удалении друг от друга должны располагаться антенны двухпозиционного СВЧ-датчика?

- 20 м;
- 50 м;
- 100 м;
- 110 м.

48. Какую концепцию применяют при проектировании нескольких линий однородного обнаружения по всей длине периметра охраняемого объекта?

- концепцию комплексной защиты;
- концепцию эшелонированной защиты;
- концепцию скрытой защиты;
- концепцию индивидуальной защиты.

49. Выберите способы, по которым классифицируют внутренние датчики охранной сигнализации:

- пассивные или активные;
- пространственные или линейные;
- действующие в пределах или вне пределов прямой видимости;
- автономные или комплексные;

50. Электромеханические датчики относят к внутренним датчикам вторжения через границу?

- да;
- нет.

51. Датчики давления относят к внутренним датчикам вторжения через границу?

- да;
- нет.

52. Инфразвуковые датчики относят к внутренним датчикам вторжения через границу?

- да;
- нет.

53. Что используется в качестве чувствительного элемента в инерционных датчиках?

- диэлектрическая пластина;
- металлический шарик;
- намагниченная проволока;

- волоконно-оптический проводник.

54. Выберите частоту, с которой пьезоэлектрический датчик обнаруживает вибрации поверхности:

- 1 - 3 КГц;
- 5 - 50 КГц;
- 70 - 100 КГц;
- 1 - 5 ГГц.

55. Какие основные элементы включает уравновешенный магнитный переключатель?

- переключатель с несколькими реле и предохранителями;
- металлический шарик, установленный на металлических контактах;
- магнитный датчик с дополнительным постоянным магнитом;
- электронный переключатель без механических контактов в реле.

56. Приборы, основанные на эффекте Холла, используют в качестве магнитных переключателей?

- да;
- нет.

57. В датчиках непрерывности вместо электрической проволоки применяют оптическое волокно?

- да;
- нет.

58. В каких датчиках для обнаружения используется метод спекл-структур?

- волоконно-оптический датчик непрерывности;
- пассивный инфразвуковой датчик;
- активный микроволновый датчик;
- волоконно-оптический датчик микроизгибов.

59. Ультразвуковые датчики относят к внутренним датчикам обнаружения движения?

- да;
- нет.

60. В каком диапазоне волн формируется поле обнаружения ультразвуковых датчиков?

- 1 - 5 КГц;
- 10 - 15 КГц;
- 19 - 40 КГц;
- 50 - 100 КГц.

61. С какой длиной волны воспринимают электромагнитное излучение пассивные инфракрасные датчики?

- 1-5 мкм;
- 8-14 мкм;
- 15-20 мкм;
- 22-34 мкм.

62. Выберите факторы, которые будут влиять на чувствительность ёмкостных датчиков?

- перемещение металлических предметов;
- изменение температуры окружающей среды;
- изменение влажности воздуха;
- освещённость охраняемых объектов.

2-е тестирование:

1. Замкнутые телевизионные системы применяют для оценки сигнала тревоги?

- да;
- нет.

2. Устройство считывания данных с персональных индивидуальных карточек входит в подсистему оценки сигнала тревоги?

- да;
- нет.

3. Устройство видеозаписи входит в подсистему оценки сигнала тревоги?

- да;
- нет.

4. Выберите типы камер, применяемых в замкнутых телевизионных системах:

- тепловизионные;
- с электронно-оптическим преобразователем;
- барометрические;
- твердотельные.

5. Что понимается под чувствительностью камеры в замкнутой телевизионной системе?

- отношение апертуры объектива к фокусному расстоянию;
- количество света, необходимого для формирования полезного сигнала;
- отношение коэффициента усиления видеосигнала к полосе пропускания;
- минимальная освещённость, необходимая для получения выходного сигнала с заданными характеристиками.

6. Тип источника искусственного освещения влияет на формирование телевизионного сигнала?

- да;
- нет.

7. Спектральная характеристика источника света влияет на формирование телевизионного сигнала?

- да;
- нет.

8. Апертура объектива телевизионной камеры влияет на формирование телевизионного сигнала?

- да;
- нет.

9. Выберите используемые источники искусственного освещения:

- светодиоды;
- люминесцентные лампы;
- биохимические смеси;
- натриевые лампы;
- ртутные лампы;
- плазмоиды.

10. Выберите заданный номинальный ресурс для ртутных ламп:

- 1000 часов;
- 6000 часов;
- 12000 часов;
- 24000 часов.

11. Выберите заданный номинальный ресурс для металлогалогенных ламп:

- 1000 часов;
- 6000 часов;
- 12000 часов;
- 24000 часов.

12. Что представляет собой система сбора данных о тревоге и их отображения (ССДО)?

- компонент системы физической защиты, передающий информацию о тревоге для её оценки на центральный пост управления и представляющий эту информацию оператору;
- совокупность источников для обнаружения несанкционированных действий нарушителя и формирования сигнала тревоги;
- механико-электрические и процедурные характеристики интерфейса при передаче информации из одного места в другое;

- передающая среда для сбора данных о тревоге с использованием электромагнитных сигналов, распространяющихся от передатчика к приёмнику с заданными характеристиками.

13. Подсистема контроля и обеспечения безопасности линий связи входит в систему сбора данных о тревоге и их отображения (ССДО)?

- да;
- нет.

14. Подсистема идентификации индивидуальных признаков персонала входит в систему сбора данных о тревоге и их отображения (ССДО)?

- да;
- нет.

15. Подсистема оценки работоспособности оборудования входит в систему сбора данных о тревоге и их отображения (ССДО)?

- да;
- нет.

16. Что понимается под термином охрана объекта?

- совокупность средств, методов и процедур, предназначенных для защиты информации на охраняемом объекте;
- размещённый на охраняемой территории персонал, обязанный реагировать на конкретные случаи нарушений;
- весь персонал службы безопасности, который может быть задействован на охраняемом предприятии, независимо от того где он находится, на самом объекте или вне его;
- кнопка тревожной сигнализации на охраняемом объекте.

17. Что понимается под термином силы реагирования охраняемого объекта?

- боеготовые формирования, предназначенные для решения внезапно возникающих задач в различных регионах мира;
- размещённый на охраняемой территории персонал, обязанный реагировать на конкретные случаи нарушений;
- весь персонал службы безопасности, который может быть задействован на охраняемом предприятии, независимо от того где он находится, - на самом объекте или вне его;
- совокупность средств, методов и процедур, предназначенных для защиты информации на охраняемом объекте.

18. Выберите основные компоненты, которые входят в функцию реагирования:

- упреждение угроз;
- своевременный ответ;

- подбор кадров;
- возврат постфактум.

19. Выберите стратегии действий, которые используют силы реагирования:

- планирование;
- блокирование;
- выжидание;
- отпор.

20. Выберите виды планирования действий сил реагирования, которые применяют в чрезвычайных ситуациях на охраняемых объектах:

- предварительное планирование;
- тактическое планирование;
- оперативное планирование;
- детальное планирование.

21. Какое максимальное расстояние надёжной связи обеспечивается между двумя маломощными переносными рациями, работающими на батарейках?

- 0,5 – 1,2 км;
- 1,5 - 5 км;
- 7 - 9 км;
- 10 - 12 км.

22. Выберите группы, в которые сведены классы защищённости автоматизированных систем обработки информации и требования к ним:

- системы, в которых работает один пользователь, допущенный ко всей обрабатываемой и хранимой информации;
- системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей обрабатываемой и хранимой информации;
- системы, в которых не работает ни один пользователь, который имеет права доступа ко всей обрабатываемой и хранимой информации;
- многопользовательские системы, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности, и различные пользователи имеют разные права на доступ к информации.

23. Требования к защите систем обработки и хранения информации могут возрастать?

- от класса 1А до 3Б;
- от класса 3Б до 1А;
- не возрастают.

24. Выберите группы, в которые сведены классы защищённости средств вычислительной техники от несанкционированного доступа к информации:

- группа минимальной защиты;

- группа избирательной защиты;
- группа системной защиты;
- группа полномочной защиты;
- группа верифицированной защиты;
- группа комплексной защиты.

25. Выберите основные методологические подходы к оценке уязвимости информации, которые сложились в процессе развития теории и практики защиты информации:

- эмпирический;
- теоретический;
- комплексный;
- теоретико-эмпирический.

26. Выберите компоненты, от которых зависит определение ожидаемых потерь при эмпирической зависимости:

- коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;
- коэффициент, характеризующий значение возможного ущерба при возникновении соответствующей угрозы;
- коэффициент, характеризующий возможные затраты для обеспечения требуемого уровня защищённости информации;
- коэффициент, характеризующий возможную частоту ложных тревог при обнаружении нарушителя.

27. Какая предпосылка взята за исходную при построении модели с полным перекрытием?

- система обработки данных, как система множественного доступа, должна иметь механизмы разграничения доступа к определённым её ресурсам;
- в механизме защиты должно содержаться, по крайней мере, одно средство для перекрытия любого потенциально возможного канала утечки информации;
- средства защиты должны оказывать какое-либо противодействие проявлению дестабилизирующих факторов при их нежелательном воздействии на защищаемую информацию.
- система защиты должна соответствовать требованиям комплексного подхода в решении задач при организации построения сложных систем.

28. Количественная мера отношения соответствующей угрозы к соответствующему защищаемому объекту определяется в методике описания системы с полным перекрытием?

- да;
- нет.

29. Определяется ли качество защищаемых ресурсов, доступ к которым должен осуществляться при предъявлении соответствующих полномочий, в методике описания системы с полным перекрытием?

- да;
- нет.

30. Выберите основные рекомендации по применению моделей с целью обеспечения решения задач анализа, синтеза и управления в системах защиты информации:

- модели могут строиться на основе несуществующих и непроверенных методов и принципов исследования;

- моделями должны пользоваться квалифицированные специалисты-профессионалы;

- модели надо использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании существенно значимыми исходными данными в возможных диапазонах их изменений;

- результаты моделирования не могут служить определённым инструментом при проведении деловых игр по защите информации;

- для оценки адекватности моделей, исходных данных и получаемых решений надо как можно шире привлекать квалифицированных и опытных экспертов;

- для эффективного использования моделей надо непрерывно уточнять исходные данные для моделирования и периодически их оценивать.

31. В каком руководящем документе содержится систематизированный каталог требований к безопасности информационных технологий, а также методические рекомендации по заданию требований при разработке, оценке и сертификации по требованиям безопасности продуктов и систем обработки информации?

- кодекс установившейся практики для менеджмента информационной безопасности;

- общие критерии;

- закон об авторском праве и смежных правах;

- закон о техническом регулировании.

32. Что понимается под безопасностью информационных технологий?

- общие требования для некоторого типа продуктов, систем и информационных технологий, представленные в виде обособленной структуры, именуемой профилем защиты, прошедшие оценку в установленном порядке и

- зарегистрированные в каталоге профилей защиты;

- уровень стойкости системы безопасности или объектов оценки, на которых предоставляется адекватная защита от случайного нарушения безопасности нарушителями с низким потенциалом нападения;

- состояние информационных технологий, определяющее защищённость информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность технологий выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений;

- приёмы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

33. Какова структура требований безопасности информации и информационных технологий в виде иерархии и содержательных наборов конструкций известной пригодности, которые могут быть использованы при установлении требований к перспективным продуктам и системам?

- задание – профиль - элемент;
- класс – семейство - компонент;
- каталог – семейство - понятие;
- уровень – узел - элемент.

34. Какой термин применяется для наиболее общего группирования требований безопасности?

- каталог;
- семейство;
- уровень;
- класс.

35. Какой термин применяется для обозначения группы наборов требований безопасности, имеющих общие цели, но различающиеся акцентами или строгостью?

- каталог;
- семейство;
- уровень;
- класс.

36. Какой термин применяется для описания специфического набора требований безопасности, являющегося наименьшим выбираемым набором требований для включения в другие структуры?

- элемент;
- понятие;
- компонент;
- узел.

37. Какой термин применяется для выражения требований безопасности на самом нижнем уровне иерархии, который может быть верифицирован при оценке продуктов и систем?

- элемент;
- понятие;

- компонент;
- узел.

38. Что понимается под стратегией защиты информации?

- условия, определяемые уровнем структурно-организационного построения объекта обработки информации, уровнем организации технологических схем обработки, местом и условиями расположения объекта и его компонентов, а также другими параметрами;

- общая, рассчитанная на перспективу, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов;

- выбор основных и наиболее важных базовых системно-концептуальных положений и ориентиров при планировании, разработке и реализации информационной деятельности;

- общий, недетализированный план какой-либо деятельности, охватывающий длительный период времени или способ достижения сложной цели.

39. Поиск оптимального компромисса между потребностями в защите информации и необходимыми для этих целей ресурсами может быть отнесен к организации защиты информации?

- да;
- нет;

40. Выберите формулировку прямой оптимизационной задачи защиты информации и объектов:

- защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты;

- защита должна быть организована так, чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов;

- защита должна быть организована так, чтобы при минимальных ресурсах обеспечивался максимально возможный уровень защиты.

- защита должна быть организована так, чтобы при максимальных ресурсах обеспечивался минимально возможный уровень защиты.

41. Выберите основные проблемы, затрудняющие формальное решение прямой и обратной оптимизационных задач защиты информации и объектов:

- взаимозависимость объёмов и важности защищаемой информации, а также условий её хранения, обработки и использования;

- процессы защиты информации находятся в значительной зависимости от большого числа случайных и труднопредсказуемых факторов;

- среди средств защиты весьма весомое место занимают организационные меры, связанные с действиями человека;

- наличие взаимосвязи процессов обнаружения нарушителей с оценкой их действий силами охраны.

42. Выберите основные критерии, которые используются при моделировании системы физической защиты:

- вклад средств защиты в общую систему;
- степень достижения требуемого уровня защиты информации и объектов;
- степень свободы действий при организации защиты;
- эффективность – стоимость системы защиты.

43. Регламентация относится к способам защиты информации и объектов?

- да;
- нет.

44. Упреждение относится к способам защиты информации и объектов?

- да;
- нет.

45. Законодательные средства относят к формальным средствам защиты информации?

- да;
- нет.

46. Физические средства относят к неформальным средствам защиты информации?

- да;
- нет.

47. Выберите важнейшее концептуальное требование к системе защиты информации и объектов:

- требование системности;
- требование адаптируемости;
- требование адекватности;
- требование экономичности.

48. Концептуальное единство относится к общеметодологическим принципам построения архитектуры системы физической защиты информации?

- да;
- нет.

49. Экспертные оценки относятся к общеметодологическим принципам построения архитектуры системы физической защиты информации?

- да;
- нет.

50. Выберите механизмы защиты, которые включает в себя архитектура системы защиты информации с точки зрения организации её построения:

- механизм контроля системы защиты;
- механизм обеспечения защиты информации;
- управление механизмами защиты;
- общая организация работы системы защиты.

51. Для чего предназначено ядро системы физической защиты информации?

- для агрегирования системы защиты на соответствующие подсистемы;
- для декомпозиции средств и процедур защиты информации в общей системе физической защиты;
- для объединения всех подсистем в единую целостную систему, а также для организации и обеспечения управления её функционированием;
- для моделирования функций системы физической защиты и её компонентов.

52. Выберите модели, которые применяют для оценки уязвимости систем физической защиты информации и объектов:

- трёхмерная модель комплексной безопасности;
- общая модель воздействия на информацию;
- модель потенциально-возможных злоумышленных действий;
- семирубежная модель.

53. Чтобы система физической защиты обеспечила эффективную задержку нарушителя необходимо?

- чтобы время реакции охраны было больше минимального времени задержки нарушителя;
- чтобы время реакции охраны было меньше минимального времени задержки нарушителя;
- чтобы время реакции охраны было равно минимальному времени задержки нарушителя.

54. Согласно принципу своевременного обнаружения, эффективность системы физической защиты определяется?

- суммарной вероятностью обнаружения нарушителя в момент, когда у сил реагирования ещё достаточно времени для его перехвата;
- суммарной вероятностью обнаружения нарушителя до достижения им цели проникновения;
- суммарным временем прохождения пути нарушителем при достаточном времени реакции сил реагирования.

55. Что понимается под критической точкой обнаружения (КТО) нарушителя?

- точка, в которой остающееся на пути время задержки нарушителя меньше времени реакции сил реагирования;
- точка, в которой остающееся на пути время задержки нарушителя всё ещё несколько превышает время реакции сил реагирования;
- точка, в которой общее время пути нарушителя всё ещё превышает минимальное время задержки, остающееся на пути нарушителя;

56. Что понимается под вероятностью прерывания действий нарушителя?

- общая суммарная вероятность обнаружения нарушителя;
- минимальная вероятность обнаружения элементом защиты;
- суммарная вероятность обнаружения нарушителя от начала его пути до критической точки обнаружения (КТО);
- вероятность своевременного развёртывания сил реагирования.

57. Что понимается под критическим путём нарушителя?

- путь нарушителя с наименьшим временем обхода каждого элемента задержки;
- путь нарушителя, у которого наименьшая вероятность прерывания его действий;
- путь нарушителя, у которого минимальное время для задержки нарушителя;
- путь нарушителя, для которого приемлемо среднее время реакции охраны.

58. Какие модели применяют в качестве инструмента количественного анализа систем физической защиты информации и объектов:

- общая модель воздействия на информацию;
- модель оценки враждебных проникновений и действий (EASI);
- модель для анализа эффективности системы в случае силового вторжения и нападения нарушителей (FESEM);
- трёхмерная модель комплексной безопасности.

59. В самом общем виде на прагматическом уровне основное требование к защите информации и объектов определяется как?

- предотвращение угроз информации, по крайней мере, тех из них, проявление которых может привести к существенно значимым негативным последствиям;
- соблюдение заданного объёма обрабатываемой информации и характера её обработки;
- правильная организация информационно-вычислительного процесса и технологий обработки защищаемой информации в системах обработки данных;
- обеспечение соответствующих возможностей средств защиты конкретным технологиям обработки, хранения и обмена информации.

60. Структуризация поля потенциально возможных вариантов сочетаний значений факторов и условий защиты входит в общую последовательность решения задачи по определению требований к защите информации?

- да;
- нет.

61. Организация информационно-вычислительных процессов в системах обработки информации входит в общую последовательность решения задачи по определению требований к защите информации?

- да;
- нет.

62. Подсистема управления доступом входит в систему физической безопасности объектов?

- да;
- нет.

63. Подсистема формирования угроз входит в систему физической безопасности объектов?

- да;
- нет.

64. Подсистема инженерно-технической защиты входит в систему физической безопасности объектов?

- да;
- нет.

65. Подсистема личной безопасности персонала входит в систему физической безопасности объектов?

- да;
- нет.

66. На основе какой концепции должно осуществляться проектирование систем физической защиты объектов?

- системно-комплексной защиты;
- полной и эшелонированной защиты;
- частично-агрегированной защиты;
- программно-аппаратной защиты.

67. Механическая система защиты входит в интегральный комплекс защиты территории охраняемых объектов?

- да;
- нет.

68. Оборонительная система входит в интегральный комплекс защиты территории охраняемых объектов?

- да;
- нет.

69. Система устранения последствий нападения входит в интегральный комплекс защиты территории охраняемых объектов?

- да;
- нет.

70. Что является важнейшей характеристикой механической системы защиты?

- собирательные признаки системы;
- частота ложных тревог;
- время, которое требуется злоумышленнику для преодоления всех физических препятствий;
- вероятность преодоления препятствий злоумышленником.

71. Каково основное требование к системе оповещения о попытках вторжения на охраняемую территорию?

- обеспечение заданного уровня защиты и надёжности информации;
- обеспечение максимальной пропускной способности для нарушителей;
- обеспечение рациональной территориальной распределённости элементов системы оповещения;
- обеспечение максимально возможной вероятности обнаружения нарушителей и надёжности системы в сочетании с минимальной частотой ложных срабатываний.

72. Что является основой систем опознавания?

- пластиковые идентификационные карточки;
- телевизионные установки дистанционного наблюдения;
- датчики охранной сигнализации;
- голографические кодировочные системы.

73. Выберите параметры, которыми определяется эффективность подсистемы входного контроля:

- вероятность обнаружения;
- пропускная способность;
- время передачи сигнала тревоги;
- частота ошибок.

74. На чём основана работа автоматизированной системы контроля доступа на объекты?

- на виртуальной способности обнаружения нарушителя;
- на анализе идентификационных документов;

- на возможности своевременного действия сил реагирования;
- на реакции постфактум.

75. Для чего предназначены пластиковые идентификационные карточки?

- для осуществления взаимодействия человека с автоматизированной системой контроля доступа в целях идентификации субъекта системы на основе идентифицирующей и другой информации;
- для опознавания нарушителей с помощью замкнутой телевизионной системы;
- для обнаружения деструктивных действий на охраняемых объектах;
- для идентификации вредоносного электромагнитного излучения и полей.

76. Какое количество информации можно записать на 1 кв. мм. трёхмерной голограммы пластиковой идентификационной карточки при голографическом способе кодирования?

- до 1000 бит информации;
- до 100 000 бит информации;
- до 500 000 бит информации;
- до 1 млн. бит информации.

77. Что понимается под процессом эмбоссирования?

- нанесение штрих-кода на пластиковую идентификационную карту;
- нанесение голограммы на пластиковую идентификационную карту;
- тиснение или выдавливание символов на поверхности идентификационной карточки;
- нанесение полосок намагниченного материала на пластиковую идентификационную карту.

78. Выберите наиболее распространённые методы кодирования пропусков:

- с помощью магнитных полосок;
- с помощью солитонов;
- с помощью интегральных схем;
- с помощью штрих-кода;

79. Что понимается под коэрцитивной силой?

- степень устойчивости открытых позиционных шифров;
- уровень эффекта интерференции между двумя и более когерентными полями;
- уровень резонансной частоты голосового тракта человека;
- степень устойчивости магнитного материала к изменениям записанной информации при воздействии магнитного поля.

80. В чём суть технологии кодирования пластиковых идентификационных карточек при помощи проволочек Виганда?

- код создаётся последовательностью нанесенных штрихов с изменяющейся шириной и расстоянием между ними;
- код создаётся сериями параллельных, встроенных в материал карты отрезков металлической проволоки с особыми магнитными свойствами;
- код создаётся с помощью специальных полосок намагниченного материала на пластиковой идентификационной карточке;
- код создаётся с помощью эффекта интерференции между двумя или более когерентными полями.

1.2. Типовые вопросы, выносимые на экзамен

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”.

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

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

**ОСНОВЫ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ СПЕЦИАЛЬНЫХ
РАБОТ ПО ВЫЯВЛЕНИЮ ЗАКЛАДОЧНЫХ УСТРОЙСТВ
(ООО «НОВО», НТЦ «ЗАРЯ»)**

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

- Сформировать представление у студентов по системам физической защиты информационных объектов и методике их применения.
- Получить первичные навыки по анализу перспектив развития подобных систем защиты.

Задачи дисциплины:

- Ознакомление студентов с методологическими подходами построения и эксплуатации систем физической защиты информационных объектов, а также с основными методами определения параметров, характеристик и структуры систем физической защиты информации;
- Формирование у студентов способности самостоятельно решать поставленные задачи в области проектирования систем физической защиты информации с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических занятий

Тема 1. Основы физической защиты информации при использовании вычислительной техники и информационных технологий.

Практическое занятие 1.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по вопросам применения вычислительной техники и информационных технологий в организации физической защиты информационных объектов.

Основные положения темы занятия:

- Возможные каналы утечки информации, характеристика компьютерных инфекций.
- Уязвимые места для утечки информации в компьютерных сетях. Основы физической защиты информации от электронного и программного воздействия.

Учебные вопросы:

1. Характеристика каналов утечки информации и их физические показатели.

2. Особенности физической среды распространения информации.
 3. Анализ информации на предмет её ценности, виды потерь информации.
- Учебное время: 4 часа.

Тема 2. Анализ угроз информационной безопасности для охраняемых объектов, каналы утечки информации и их классификация.
Практическое занятие 2.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по анализу угроз информационной безопасности для охраняемых объектов.

Основные положения темы занятия:

- Источники угроз, объективные и субъективные предпосылки их появления.
- Основные мероприятия по защите информационных объектов от утечки информации по различным каналам и полям.

Учебные вопросы:

1. Фундаментальные угрозы утечки информации, нарушение целостности данных, отказ в обслуживании и незаконное использование привилегий.
2. Первичные угрозы в качестве проникновения на объекты (маскарад, обход защиты, нарушение полномочий) и внедрение технических средств съёма информации.
3. Потенциальные виды угроз и модель нарушителей информационных объектов.

Учебное время: 4 часа.

Тема 3. Основные функции и элементы системы физической защиты и их особенности.

Практическое занятие 3.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по определению основных функций и элементов физической защиты объектов.

Основные положения темы занятия:

- Взаимосвязь между функциями и элементами защиты.
- Архитектура системы защиты информации, требования к ней, порядок построения систем физической защиты, основные стратегии защиты.

Учебные вопросы:

1. Взаимосвязь между функциями и процедурами системы физической защиты.
2. Основные характеристики эффективной системы физической защиты и взаимодействие между ними.
3. Архитектура систем физической защиты информационных объектов, порядок проектирования и построения систем защиты.
4. Ресурсы и виды обеспечения систем физической защиты информационных объектов.

Учебное время: 4 часа.

Тема 4. Методика применения датчиков охранной сигнализации и их характеристика.

Практическое занятие 4.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по методике применения датчиков охранной сигнализации.

Основные положения темы занятия:

- Сильные и слабые стороны датчиков, особенности их установки и эксплуатации с учётом естественных и искусственных факторов воздействия.
- Характеристика окончательно спроектированной подсистемы датчиков обнаружения вторжения.

Учебные вопросы:

1. Методика применения внешних датчиков охранной сигнализации и их особенности эксплуатации.
2. Методика применения внутренних датчиков охранной сигнализации и их особенности эксплуатации.
3. Технологии совместного применения датчиков, их достоинства и недостатки.
4. Особенности проектирования подсистемы обнаружения вторжения на основе различных датчиков.

Учебное время: 4 часа.

Тема 5. Сбор данных о тревоге и их оценка. Характеристика сил реагирования.

Практическое занятие 5.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по формированию и применению сил реагирования.

Основные положения темы занятия:

- Развитие систем сбора данных о тревоге и отображения, их состав и особенности построения.
- Планирование действий сил реагирования в чрезвычайных ситуациях и порядка их использования.

Учебные вопросы:

1. Характеристика систем сбора данных о тревоге и отображения сигналов оповещения, порядок их применения.
2. Безопасность системы сбора данных о тревоге и оповещения, характеристики совместно используемых компонентов.
3. Порядок формирования и применения сил реагирования на охраняемых объектах.
4. Организация связи на охраняемых объектах, характеристики современных средств связи.

Учебное время: 4 часа.

Тема 6. Моделирование процессов применения систем физической защиты информации.

Практическое занятие 6.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по моделированию процессов применения систем физической защиты объектов.

Основные положения темы занятия:

- Понятие модели защиты информации. Модель защиты как модель системы с полным перекрытием.
- Основные критерии оценки эффективности при проектировании систем физической защиты, качественный и количественный их анализ.

Учебные вопросы:

1. Характеристика критериев и показателей оценки эффективности систем физической защиты информации.
2. Характеристика семирубежной модели защиты информационных объектов и других моделей физической защиты информации.
3. Компьютерные модели, как инструменты количественного анализа систем физической защиты информационных объектов.
4. Основы методики качественного анализа и оценки проектируемых систем физической защиты.

Учебное время: 4 часа.

Тема 7. Основные подходы и методы проектирования систем физической защиты информации.

Практическое занятие 7.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по методике проектирования систем физической защиты информационных объектов.

Основные положения темы занятия:

- Методы формирования основных функций физической защиты и выбора средств защиты.
- Проектирование основных подсистем и элементов системы физической защиты информационных объектов в соответствии с концепцией полной и эшелонированной защиты.

Учебные вопросы:

1. Формирование требований к системе физической защиты объектов.
2. Особенности проектирования подсистем и технических средств физической защиты.
3. Характеристика элементов классической системы обеспечения безопасности охраняемых объектов.
4. Пример организации физической защиты вычислительного центра, как типового охраняемого объекта.

Учебное время: 4 часа.

Тема 8. Организация безопасности информационных объектов с помощью средств физической защиты.

Практическое занятие 8.

Вид практического занятия: *смешанная форма практического занятия.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по организации безопасности информационных объектов с помощью средств физической защиты.

Основные положения темы занятия:

- Регулирование доступа на охраняемые объекты, характеристика систем контроля доступа и порядок их применения.
- Комплексное обеспечение физической защиты объектов с помощью различных систем и средств.

Учебные вопросы:

1. Порядок применения средств физической защиты информационных объектов на предприятии (в фирме).
 2. Интегральный комплекс физической защиты объекта и его основные элементы.
 3. Подсистема контроля доступа на охраняемые объекты, характеристика биометрических средств идентификации.
 4. Предназначение, структура и возможности охранных систем отечественного производства, распространённых на рынке современных средств защиты.
- Учебное время: 4 часа.

4. Указания по проведению самостоятельной работы студентов

2. Указания по проведению самостоятельной работы студентов

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

		<p>Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.</p> <p>Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.</p>
3	<p>Основные уровни защиты информации компьютерных системах</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.</p> <p>Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.</p> <p>Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.</p>
4	<p>Основные положения формальной теории защиты информации</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Перечень основных документов ФСТЭК России по вопросам защиты информации.</p> <p>Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.</p>
5	<p>Формальные модели безопасности</p>	<p>Подготовка докладов и презентаций по темам:</p> <p>Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ.</p>

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

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Информационные процессы в сфере государственного и муниципального управления.
2. Виды информации и информационных ресурсов в сфере государственного и муниципального управления.
3. Состояние и перспективы физической защиты информации в сфере государственного и муниципального управления.
4. Общие сведения о компьютерных вирусах и принципы их действия.
5. Понятие программных закладок и особенности их применения на охраняемых объектах.
6. Характеристика программных средств борьбы с вирусами и программными закладками, особенности их применения на охраняемых объектах.
7. Характеристика компьютерных моделей как инструмента количественного анализа систем защиты информации и объектов.
8. Порядок построения диаграмм последовательности действий нарушителя.
9. Основные подходы к управлению рисками в процессе оценки уязвимости охраняемых объектов.
10. Проблемы физической защиты информации в сфере государственного и муниципального управления.
11. Защита информации в вычислительных системах и средах.
12. Применение компьютерных моделей для оценки эффективности проектируемых систем физической защиты информации и объектов.
13. Основные подходы к применению систем физической защиты информации за рубежом на государственном и ведомственном уровнях.

Примерные темы докладов

1. Состав и основные характеристики современных систем и средств контроля и управления доступом.
2. Особенности применения современных средств охранной сигнализации в России и за рубежом.
3. Состав и основные характеристики современных средств охранной сигнализации.
4. Особенности применения современных систем и средств контроля и управления доступом в России и за рубежом.
5. Состав и основные характеристики современных радиоволновых однопозиционных средств охраны.
6. Особенности применения современных радиоволновых однопозиционных средств охраны в России и за рубежом.
7. Состав и основные характеристики современных радиоволновых двухпозиционных средств охраны.
8. Особенности применения современных радиоволновых двухпозиционных средств охраны в России и за рубежом.

9. Состав и основные характеристики современных проводноволновых средств охраны.
10. Особенности применения современных проводноволновых средств охраны в России и за рубежом.
11. Состав и основные характеристики современных вибрационных средств охраны.
12. Особенности применения современных вибрационных средств охраны в России и за рубежом.
13. Состав и основные характеристики современных сейсмических средств охраны.
14. Особенности применения современных сейсмических средств охраны в России и за рубежом.
15. Состав и основные характеристики современных магнитометрических средств охраны.
16. Особенности применения современных магнитометрических средств охраны в России и за рубежом.
17. Состав и основные характеристики современных оптико-электронных однопозиционных средств охраны.
18. Особенности применения современных оптико-электронных однопозиционных средств охраны в России и за рубежом.
19. Состав и основные характеристики современных ёмкостных средств охраны.
20. Особенности применения современных ёмкостных средств охраны в России и за рубежом.

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 технического 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 для освоения дисциплины (модуля)

Основная литература:

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/237770> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2. Алёшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алёшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167600> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Система охраны государственной тайны : учебное пособие / составители Е. 3.Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 138 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/261902> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

4. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. — Новосибирск : СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/222380> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности.
– Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».

6. <http://www.academy.it.ru/> – академия АЙТИ.
 7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
 8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.
 9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
- <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: *MOffice, PowerPoint.*

Информационные справочные системы:

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