МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Инженерно-техническая защита информации
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации Д.А. Митюшин
……..
Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры КЗИ
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование знаний и навыков в области методов и технологий инженерно-технической защиты информации, составляющей государственную тайну, обрабатываемую в системах информатизации в защищённом исполнении (СИЗИ).

Задачи дисциплины:

дать знания:

– о нормативных правовых актах, нормативными методическими документами ФСТЭК России и Росгвардии в области инженерно-технической защиты информации ограниченного доступа;

– об основах инженерно-технической защиты информации ограниченного распространения;

– об основах проведения специальных проверок, специальных исследований и специальных обследований;

– об основах аттестации объектов информатизации на соответствие требованиям по защите информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-2 – Способен оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов	ПК-2.1 – Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД	Знать: нормативные правовые акты, методические документы ФСТЭК России и Росгвардии, национальные стандарты в области инженерно-технической защиты информации ограниченного доступа, проектирования и сертификации средств инженерно-технической защиты информации на соответствие требованиям по безопасности информации, аттестации объектов информатизации на соответствие требованиям по защите информации.
	ПК-2.2 – Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищённом исполнении	Уметь: оформлять рабочую и эксплуатационную документацию на средства и системы инженерно-технической защиты информации объекта информатизации
	ПК-2.3 – Владеет навыками разработки технического проекта средства и/или системы информатизации в защищённом исполнении	Владеть: навыками разработки технического проекта систем инженерно-технической защиты информации, акта обследования объекта защиты

ПК-5 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	ПК-5.1 – Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации	Знать: процедуру организации установки и настройки средств инженерной, технической защиты информации, защиты информации от утечки по технически каналам в соответствии с техническим проектом и инструкциями по эксплуатации
	ПК-5.2 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	Уметь: разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы инженерно-технической защиты информации
	ПК-5.3 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Владеть: навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Инженерно-техническая защита информации» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: дисциплина является дисциплиной начального цикла обучения.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Спецкурс № 3 (ДСП)», «Проектно-технологическая практика» и «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов,

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
1	Лекции	28
1	Семинары/лабораторные работы	36
Всего:		64

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _44_ академических часа.

3. Содержание дисциплины

Тема 1. Общие положения инженерно-технической защиты информации

Основные нормативные документы, термины и определения инженерно-технической защиты информации. Рубежи защиты.
Угрозы безопасности информации. Классификация угроз.
Основные принципы инженерно-технической защиты информации.

Тема 2. Технические каналы утечки информации

Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков объектов защиты.
Опасные сигналы и их источники.
Побочные электромагнитные излучения и наводки.
Особенности утечки информации. Типовая структура и виды технических каналов утечки информации.
Основные принципы разведки. Связь с принципами защиты информации. Классификация технической разведки.
Средства добывания информации. Классификация технических средств разведки.

Тема 3. Системы инженерной защиты. Инженерно-техническая укреплённость объектов информатизации

Модель угроз и модель нарушителя безопасности информации.
Подсистема физической защиты информации. Комплекс инженерной защиты источников информации. Классификация инженерных средств охраны.
Инженерно-техническая укреплённость. Классификация и назначение средств инженерно-технической укреплённости.
Классификация объектов охраны.

Тема 4. Технические средства охраны

Нормативные документы по техническим средствам охраны.
Классификация технических средств охраны. Рубежи охраны.
Извещатели, классификация извещателей системы охраны. Извещатели систем пожарной сигнализации.
Системы охраны периметра. Объектовые системы охраны.
Системы видеонаблюдения.

Интегрированные системы охраны.

Тема 5. Системы контроля и управления доступом

Нормативные документы по системам контроля и управления доступом (СКУД).
Классификация средств и систем КУД.
Идентификаторы. Контроллеры. Методы и средства аутентификации и идентификации личности. Исполнительные устройства. Методы и средства биометрии.

Тема 6. Противодействие утечке информации по техническим каналам

Методы противодействия наблюдению. Методы противодействия наблюдению в оптическом диапазоне. Методы противодействия радиолокационному наблюдению.
Методы противодействия подслушиванию. Структурное скрытие речевой информации в каналах связи. Энергетическое скрытие акустического сигнала.
Обнаружение и подавление закладных устройств. Демаскирующие признаки закладных устройств. Методы обнаружения закладных подслушивающих устройств. Методы подавления подслушивающих закладных устройств. Способы контроля помещений на отсутствие закладных устройств.
Экранирование побочных излучений и наводок.
Методы предотвращения утечки информации по вещественному каналу.

Тема 7. Аттестация объектов информатизации

Основные понятия в области аттестации объектов информатизации.
Правовая и методическая основа аттестации объектов информатизации.
Спецпроверка, специсследование и спецобследование.
Место и роль аттестации объектов информатизации в системе защиты информации.
Структура системы аттестации объектов информатизации.
Порядок проведения аттестации объекта информатизации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	*Тема 1. Общие положения инженерно-технической защиты информации*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой* *Консультирование и проверка заданий посредством электронной почты*
2	*Тема 2. Технические каналы утечки информации*	*Лекция 2.1* *Лекция 2.2* *Лекция 2.3* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой* *Консультирование и проверка заданий посредством электронной почты*
3	*Тема 3. Системы инженерной защиты. Инженерно-техническая укреплённость объектов*	*Лекция 3.1* *Лекция 3.2*	*Традиционная лекция с использованием презентаций*

	информатизации	*Самостоятельная работа*	*Работа с литературой Консультирование и проверка заданий посредством электронной почты*
4	*Тема 4. Технические средства охраны*	*Лекция 4.1 Лекция 4.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой Консультирование и проверка заданий посредством электронной почты*
5	*Тема 5. Системы контроля и управления доступом*	*Лекция 5.1 Лекция 5.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой Консультирование и проверка заданий посредством электронной почты*
6	*Тема 6. Противодействие утечке информации по техническим каналам*	*Лекция 6.1 Лекция 6.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой Консультирование и проверка заданий посредством электронной почты*
7	*Тема 7. Аттестация объектов информатизации*	*Лекция 7.1 Лекция 7.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой Консультирование и проверка заданий посредством электронной почты*
9	*Практическое занятие 1. Разработка модели угроз и нарушителя объекта информатизации*	*Практическое занятие 1.* *Самостоятельная работа*	*Выполнение и защита практического задания*
10	*Практическое занятие 2. Разработка макета интегрированной системы охраны объекта информатизации*	*Практическое занятие 2.* *Самостоятельная работа*	*Выполнение и защита практического задания*
11	*Практическое занятие 3. Поиск радиозакладных устройств с использованием индикаторов поля*	*Практическое занятие 3.* *Самостоятельная работа*	*Выполнение и защита практического задания*
12	*Практическое занятие 4. Поиск закладных устройств с использованием систем*	*Практическое занятие 4.* *Самостоятельная*	*Выполнение и защита практического задания*

	нелинейной локации	*работа*	
13	*Практическое занятие 5 Подавление систем радиосвязи в отдельно взятом помещении*	*Практическое занятие 5.* *Самостоятельная работа*	*Выполнение и защита практического задания*
14	*Практическое занятие 6 Разработка документов для проведения аттестации объекта информатизации*	*Практическое занятие 6.* *Самостоятельная работа*	*Выполнение и защита практического задания*

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Максимальное количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос или тестирование* *- практическое занятие 1* *- практические занятия 2-6*	 *3 балла* *4 балла* *7 баллов*	 *21 балл* *4 балла* *35 баллов*
Промежуточная аттестация – *зачёт с оценкой*		*40 баллов*
Итого за семестр		*100 баллов*

Полученный совокупный результат (максимум 100 баллов) конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые
67-50/ D,E	удовлетвори тельно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлетво рительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и

рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос
1.	Структура технического канала утечки информации, особенности утечки информации, утечки информации по техническим каналам.
2.	Характеристики составных элементов технического канала утечки информации (носители информации, средства передачи, приёма сигналов, среда передачи сигнала).
3.	Случайные антенны, понятия, технические характеристики, виды излучателей электромагнитных колебаний.
4.	Преобразователи акустического сигнала в радиоэлектронный, физические основы, активные и пассивные преобразователи акустического сигнала
5.	Физические основы возникновение паразитных связей и наводок в электрических цепях.
6.	Виды технических разведок, преимущества технических разведок в сравнении с иными видами разведок по добыванию информации.
7.	Эффективность ведения технической разведки, принципы ведения (активность, целеустремлённость скрытность, безопасность и т.п.), показатели технической разведки по добыванию защищаемой информации (достоверность, полнота, безопасность и материальные затраты).
8.	Методы доступа («заходовый», «беззаходовый» на объект защиты) к защищаемой информации, понятие и образование разведывательного контакта.
9.	Цели и задачи специальной проверки технических средств, специального обследования предметов мебели и интерьера, технических средств.
10.	Цели и задачи специального исследования технических средств, предназначенных для обработки защищаемой информации.
11.	Классификация методов, способов, технических средств защиты информации от её утечки по техническим каналам.
12.	Методы и средства пассивной (звукоизоляция и звукопоглощение) и активной (энергетического) защиты акустической (речевой) информации.
13.	Основные положения системного и комплексного подхода к построению системы охраны объекта защиты?
14.	Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия.
15.	Модель поведения нарушителя. Классификация нарушителей, физические параметры нарушителя. методы и способы реализации угроз безопасности объектов защиты.
16.	Назначение, основные задачи системы охранного видеонаблюдения. Состав и технические характеристики системы и отдельных элементов системы охранного видеонаблюдения.
17.	Видеоконтроль – как основной способ контроля доступа на объект охраны (в помещение). Организация общей системы видеоконтроля. Обработка и хранение видеозаписей.
18.	Структура системы охранного видеонаблюдения. Способы передачи видеосигнала по общим каналам связи. Разбор типовых схем телевизионных систем контроля и наблюдения.
19.	Основные принципы построения системы контроля и управления доступом по обеспечению безопасности объекта защиты.
20.	Назначение, задачи, системы контроля и управления доступом (СКУД), состав элементов СКУД и их технические характеристики.
21.	Выбор и использование биометрических систем контроля и управления доступом

	(СКУД) в зависимости от исходных данных объекта защиты.
22.	Назовите основные требования для охраны важных помещений (помещения группы Б).
23.	Назовите основные требования для охраны особо важных помещений (помещения группы А).
24.	Назовите основные классы извещателей по физическому принципу действия
25.	Что такое аттестация ОИ?
26.	Перечислите элементы структуры системы аттестации ОИ

Примерные вопросы к тестированию
(проверка сформированности компетенции ПК-2):

1. _____защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств это –

2. Какие средства включают в себя средства инженерно-технической защиты информации?
а) средства противодействия угрозам воздействия на информацию
б) средства противодействия утечке информации
в) средства противодействия хищению информации
г) средства противодействия угрозам перехвата информации

3. Каким документом утверждена Доктрина информационной безопасности Российской Федерации?
а) Федеральным законом от 27.07.2006 г. № 152-ФЗ
б) Указом Президента Российской Федерации от 05.12.2016 г. № 646
в) Постановлением Правительства РФ от 10.10.2012 г. № 1045
Ответ:
б) Указом Президента Российской Федерации от 05.12.2016 г. № 646

4. Какие виды защиты информации определяет ГОСТ Р 50922?
а) правовая
б) аппаратная
в) техническая
г) криптографическая
д) программная
е) физическая

5. _____ угрозы информационной безопасности – угрозы информационной безопасности, вызванные воздействиями на информационную систему и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

6. _____ угрозы информационной безопасности – угрозы информационной безопасности информационной системы, вызванные деятельностью человека.

7. Расположите в правильной последовательности этапы специальной проверки технического средства
разработка программы проведения специальной проверки технического средства
анализ результатов и оформление отчётных документов

проведение технических проверок
приём-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки

8. Каким нормативным документом ГУВО Росгвардии определяется инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации?
а) Методические рекомендации Р 078-2019
б) Методические рекомендации Р 063-2017
в) Методические рекомендации Р 048-2017

9. В каком нормативном документе ГУВО Росгвардии приводятся классификация объекта охраны?
а) Методические рекомендации Р 078-2019
б) Методические рекомендации Р 063-2017
в) Методические рекомендации Р 048-2017

10. К какому классу объектов охраны относятся помещения с оборотом сведений, составляющих гостайну?

11. Расположите в правильной последовательности перемещение информации по каналу утечки.
Злоумышленник
Среда распространения
Источник информации
Техническое средство приёма

Примерные вопросы к тестированию
(проверка сформированности компетенции ПК-5):

1. Чем достигается требуемый уровень безопасности информации

2. Что такое признаковая информация?

3. _____ защиты информации представляет собой заранее намеченный результат защиты информации

4. Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации это –

5. _____ защищаемой _____ – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

6. Поставить в соответствие демаскирующим признакам их характеристику.

Видовые демаскирующие признаки	Физический и химический состав, структуру и свойства веществ материального объекта
Демаскирующие	Форма объекта, его размеры, детали объекта, тон, цвет и

признаки сигналов	структура его поверхности и др.
Демаскирующие признаки веществ	Параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т.д.

7. _____ _____ – элемент средства съёма информации, скрытно внедряемый в места возможного съёма информации

8. Какой демаскирующий признак является наиболее информативным?

9. В каком интервале значений колеблется величина прямых демаскирующих признаков?

10. К каким демаскирующим признакам относятся фотометрические и геометрические характеристики объектов (форма, размеры объекта, цвет, структура, рисунок и детали его поверхности), тени, дым, пыль, следы на грунте, снегу, воде, взаимное расположение элементов группового (сложного) объекта, расположение защищаемого объекта относительно других известных объектов?

Промежуточная аттестация (зачёт с оценкой)

Примерные вопросы к **зачёту с оценкой**

№	Вопрос
1.	Основные нормативные документы, термины и определения инженерно-технической защиты информации. Рубежи защиты.
2.	Угрозы безопасности информации. Классификация угроз.
3.	Основные принципы инженерно-технической защиты информации
4.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков объектов защиты.
5.	Опасные сигналы и их источники
6.	Побочные электромагнитные излучения и наводки
7.	Особенности утечки информации. Типовая структура и виды технических каналов утечки информации.
8.	Основные принципы разведки. Связь с принципами защиты информации.
9.	Средства добывания информации. Классификация технических средств разведки.
10.	Классификация технической разведки.
11.	Модель угроз и модель нарушителя безопасности информации.
12.	Подсистема физической защиты информации. Комплекс инженерной защиты источников информации
13.	Классификация инженерных средств охраны
14.	Инженерно-техническая укреплённость. Классификация и назначение средств инженерно-технической укреплённости.
15.	Классификация объектов охраны (защиты) по нормативным документам Росгвардии
16.	Классификация технических средств охраны. Рубежи охраны.
17.	Извещатели, классификация извещателей системы охраны. Извещатели систем пожарной сигнализации.
18.	Системы охраны периметра. Объектовые системы охраны
19.	Системы видеонаблюдения. Интегрированные системы охраны
20.	Классификация средств и систем КУД
21.	Идентификаторы. Контроллеры. Методы и средства аутентификации и идентификации личности.
22.	Исполнительные устройства.

23.	Методы и средства биометрии
24.	Методы противодействия наблюдению в оптическом диапазоне.
25.	Методы противодействия радиолокационному наблюдению.
26.	Структурное скрытие речевой информации в каналах связи.
27.	Энергетическое скрытие акустического сигнала.
28.	Обнаружение и подавление закладных устройств. Демаскирующие признаки закладных устройств.
29.	Методы обнаружения закладных подслушивающих устройств. Методы подавления подслушивающих закладных устройств.
30.	Способы контроля помещений на отсутствие закладных устройств.
31.	Экранирование побочных излучений и наводок
32.	Основные понятия в области аттестации объектов информатизации.
33.	Правовая и методическая основа аттестации объектов информатизации.
34.	Спецпроверка, специсследование и спецобследование.
35.	Место и роль аттестации объектов информатизации в системе защиты информации.
36.	Структура системы аттестации объектов информатизации
37.	Порядок проведения аттестации объекта информатизации

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основные источники

1. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.
4. *Положение по аттестации* объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. (По состоянию на 8 июля 2018 г.). [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g, свободный. – Загл. с экрана.
5. *Приказ ФСТЭК России* от 29 апреля 2021 г. № 77 “Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну” [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/3075
6. *Информационное сообщение ФСТЭК России* от 29 апреля 2021 г. № 240/24/2087 Об утверждении порядка аттестации объектов информатизации и особенностях его реализации Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/2974
7. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс] : Режим

доступа : http://gostrf.com/normadata/1/4294818/4294818891.pdf, свободный. – Загл. с экрана.
8. Рекомендации стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. [Электронный ресурс] : Режим доступа : http://gostrf.com/normadata/1/4293850/4293850561.pdf, свободный. – Загл. с экрана.
9. Методические рекомендации Р 078-2019. «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2019. – 58 с. [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
10. Рекомендации Р 78.36.002-2010 «Выбор и применение систем охранных телевизионных». – М.: ФГУ НИЦ «Охрана» МВД России, 2010, – 183 с. [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
11. Методические рекомендации Р 063-2017 «Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФГУ НИЦ «Охрана» Росгвардии, 2017, – 50 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

Дополнительные источники

12. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/296, свободный. – Загл. с экрана.
13. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/297, свободный. – Загл. с экрана.
14. *Приказ ФСТЭК России* от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/566 – Загл. с экрана.
15. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/561. – Загл. с экрана.
16. ТП 78.36.001-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Комната хранения оружия». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
17. ТП 78.36.002-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
18. ТП 78.36.003-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Трёхкомнатная квартира». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

19. ТП 78.36.004-2014 Типовой рабочий проект «Система охранного телевидения». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
20. ТП 78.36.005-2014 Типовой рабочий проект «Система контроля и управления доступом. Административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

Основная литература

1. *Тумбинская, М. В.* Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург : Лань, 2022. — 344 с. – ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095 -- Режим доступа: для авториз. пользователей.
2. *Торокин А.А.* Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 958 с.
3. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. – Пермь : ПНИПУ, 2007. – 340 с. – ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366. – Режим доступа: для авториз. пользователей.

Дополнительная литература

4. *Рагозин, Ю. Н.* Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103203. — Режим доступа: для авториз. пользователей..

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : URL: https://bdu.fstec.ru/threat, свободный. – Загл. с экрана.
2. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.
3. Онлайн-курс «Аттестация объектов информатизации по требованиям безопасности информации» Автор: Ольга Сапронова. [Электронный ресурс] : Режим доступа : https://www.intuit.ru/studies/courses/3648/890/info свободный. – Загл. с экрана.
4. Национальная электронная библиотека (НЭБ) www.rusneb.ru
5. ELibrary.ru Научная электронная библиотека www.elibrary.ru
6. Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

1. Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащён

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2013	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Для проведения ряда практических занятий – специализированный класс с компьютерами и следующее оборудование

1. Индикаторы поля ST007 или аналог – 2 ш.
2. Макеты РЗУ – 2 шт.
3. Имитатор РЗУ – 1 шт.
4. Нелинейный локатор – 1…2 ш.
5. Подавитель радиосвязи «Терминатор-2000» – 1 шт.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1

Тема – ***Разработка модели угроз и нарушителя объекта информатизации***

Задания:

1. Построить вербальную модель объекта защиты для указанного преподавателем помещения.
2. Описать объект защиты, предположительные каналы утечки информации,
3. Описать модель поведения внешнего и внутреннего нарушителей, методы, способы и технические средства съёма информации, методы, способы и технические

решения по защите информации от её утечки по каналу утечки информации, указанному преподавателем.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме, нормативные документы ФСТЭК России.
2. Преподавателем выдаётся описание помещзения
3. Составить отчёт о выполнении практического задания
4. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Windows 10 Pro и Microsoft Office 2010.

Практическое занятие 2

Тема – *Разработка макета интегрированной системы охраны объекта информатизации*

Задания:

1. Изучить выданные в электронном виде:
   - требования рекомендаций ГУВО Росгвардии Р-078-2019 и Р-063-2017;
   - форму и пример составления акта обследования состояния технической укреплённости объекта (Р-063-2017).
2. Изучить выданные варианты планировок объектов с техническими описаниями их элементов технической укреплённости (в электронном виде, всего 17 вариантов) и нарисовать план защищаемого помещения.
3. На основании Р-078-2019, и Р-063-2017 примера акта обследования, руководствуясь вышеуказанными требованиями по оформлению и содержанию актов, примером акта, определить категорию объекта и составить акт обследования состояния инженерно-технического укрепления объекта.
4. Изучить технические характеристики современных технических средств охраны производства НВП «Болид» (https://bolid.ru) и ЗАО «Риэлта», г. Санкт-Петербург (https://rielta.ru)
5. На основании РД Р-078-2019, изученного лекционного материала и примера составления проектной документации (выданного в электронном виде) составить по имеющимся вариантам планировок, составленных в п.2, структурную схему, поэтажные планы сетей ОТС, пояснительную записку, расчёт ёмкости резервного питания, спецификацию оборудования.
6. 4.2. При использовании технических средств охраны применять оборудование НВП «Болид» и ЗАО «Риэлта» г. Санкт-Петербург. (Возможно использование других технических средств по согласованию с преподавателем).
7. Выбрать СКУД и видеокамеры с сайта https://bolid.ru/production/cctv/network_camera/ с учётом места установки (условий работы) и разместить видеокамеры на схеме объекта с учётом охраны внешнего периметра здания.
8. Рассчитать поля зрения камер и минимальную разрешаемую деталь для каждой камеры и сделать вывод о том, следует ли оставить эту камеру или изменить параметры объектива.
9. Выбрать регистраторы с раздела сайта https://bolid.ru/production/cctv/nvr/ и коммутаторы с раздела https://bolid.ru/production/cctv/switche/.
10. Необходимое количество регистраторов разместить на посту охраны. Коммутаторы на этажах на стойках.
11. Нарисовать схему системы охранного телевидения объекта (ТК, необходимое количество коммутаторов и регистраторов).
12. Рассчитать ёмкость каждого видеорегистратора с учётом его ТТХ.

13. Составить отчёт о работе, в котором должны быть приведены план-схема объекта и акт об осмотре объекта с рекомендациями об ИТУ объекта..

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Преподаватель раздаёт в электронном виде рекомендации ГУВО Росгвардии Р-078-2019 и Р-063-2017, описания помещений и поэтажные схемы помещений (как вариант – студенты сами рисуют планы в MS Visio).
3. Преподаватель раздаёт в электронном виде:
   - примеры проектной документации (листы проекта, поэтажные планы, структурная схема, пояснительная записка) и типовой проект ТП 78.36.004-2014 в электронном виде;
   - варианты планировок объектов с техническими описаниями их элементов технической укреплённости, применяемые в работе № 1.
4. При составлении плана помещений и схемы охраны использовать MS Visio, стандартные условные обозначения извещателей и на выбор радиальное распределение шлейфов или двухпроводную адресную линию.
5. Ответить на теоретические вопросы при защите отчёта о практическом занятии.

Материально-техническое обеспечение занятия:

1. Компьютеры *по* количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, включая MS Visio.
2. Развёрнутые *виртуальные* машины в количестве 2 шт. на каждом ПК с ОС Linux и Windows

Практическое занятие 3

Тема – *Поиск радиозакладных устройств с использованием индикаторов поля*

Задания:

1. С помощью индикаторов поля осуществить поиск макетов и имитаторов радиозакладных устройств (РЗУ).
2. При обнаружении РЗУ провести фотографирование «закладки» в месте установки, изъять её и провести фотографирование внешнего вида.
3. Составить протокол (акт) обнаружения РЗУ, который включить в отчёт.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изделия включать согласно инструкции по эксплуатации.
3. Составить отчёт о практическом занятии.
4. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

6. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010
7. Индикаторы поля ST007 или аналог – 2 ш.
8. Макеты РЗУ – 2 шт.
9. Имитатор РЗУ – 1 шт.

Практическое занятие 4

Тема – *Поиск закладных устройств с использованием систем нелинейной локации*

Задания:

1. С помощью нелинейного локатора осуществить поиск макетов и имитаторов закладных устройств (ЗУ).
2. При обнаружении ЗУ провести фотографирование «закладки» в месте установки, изъять её и провести фотографирование внешнего вида.
3. Составить протокол (акт) обнаружения ЗУ, который включить в отчёт.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изделия включать согласно инструкции по эксплуатации.
3. В качестве имитаторов ЗУ могут использоваться микросхемы.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010
2. Нелинейный локатор – 1…2 ш.
3. Макеты РЗУ – 2 шт.
4. Имитатор ЗУ – 1 шт.

Практическое занятие 5

Тема – *Подавление систем радиосвязи в отдельно взятом помещении*

Задания:

1. С помощью подавителя радиосредств осуществить подавление в пределах класса с использованием круговых и направленных антенн:
   - мобильных телефонов стандарта 3G и 4G;
   - сигналов спутниковой связи (GPS);
   - голосовой связи по мобильным телефонам и SMS-сообщений;
   - канала связи Bluetooth между устройствами.
2. Зафиксировать радиус подавления, в т.ч. за пределами аудитории.
3. Сделать скриншоты (фотографии) изменений в работе мобильных устройств.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изделия включать согласно инструкции по эксплуатации.
3. Составить отчёт о практическом занятии.
4. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010
2. Подавитель радиосвязи «Терминатор-2000» – 1 шт.

Практическое занятие 6

Тема – *Разработка документов для проведения аттестации объекта информатизации*

1. Разработать заявку для проведения аттестации объекта информатизации предложенной организации по следующей форме

Кому:_____
(наименование органа по аттестации и его адрес)

З А Я В К А
на проведение аттестации объекта информатизации

1. *(наименование заявителя)* просит провести аттестацию *(наименование объекта информатизации)* на соответствие требованиям по безопасности информации:_____

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____

5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____

5.3. Испытания несертифицированных средств и систем информатизации *(наименование средств и систем)* предусмотрено провести в испытательных центрах (лабораториях) *(наименование испытательных центров)* в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____)

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

Приложение к форме "Заявки..."

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов

1. Полное и точное наименование объекта информатизации и его назначение.

2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).

3. Организационная структура объекта информатизации.

4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).

5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

8. Наличие и характер взаимодействия с другими объектами информатизации.

9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.

10. Перечень технических и программных средств в защищённом исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому студенту структуру и штат организации.
2. Студенты должны определить территориальный орган ФСТЭК России и орган по аттестации, ближайший к организации, аккредитованной во ФСТЭК России.

Список литературы:

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. . [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g, свободный. – Загл. с экрана.
2. Онлайн-курс «Аттестация объектов информатизации по требованиям безопасности информации» Автор: Ольга Сапронова). [Электронный ресурс] : Режим доступа : https://www.intuit.ru/studies/courses/3648/890/info свободный. – Загл. с экрана

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office

Приложение 1

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Инженерно-техническая защита информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: формирование знаний и навыков в области методов и технологий инженерно-технической защиты информации, составляющей государственную тайну, обрабатываемую в системах информатизации в защищённом исполнении (СИЗИ).

Задачи: дать знания: о нормативных правовых актах, нормативными методическими документами ФСТЭК России и Росгвардии в области инженерно-технической защиты информации ограниченного доступа; об основах инженерно-технической защиты информации ограниченного распространения; об основах проведения специальных проверок, специальных исследований и специальных обследований; об основах аттестации объектов информатизации на соответствие требованиям по защите информации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-2 – Способен оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов
  ПК-2.1 – Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД
  ПК-2.2 – Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищённом исполнении
  ПК-2.3 – Владеет навыками разработки технического проекта средства и/или системы информатизации в защищённом исполнении
- ПК-5 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации
  ПК-5.1 – Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
  ПК-5.2 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
  ПК-5.3 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

В результате освоения дисциплины обучающийся должен:
Знать: нормативные правовые акты, методические документы ФСТЭК России и Росгвардии, национальные стандарты в области инженерно-технической защиты информации ограниченного доступа, проектирования и сертификации средств инженерно-технической защиты информации на соответствие требованиям по безопасности информации, аттестации объектов информатизации на соответствие требованиям по защите информации; процедуру организации установки и настройки средств инженерной, технической защиты информации, защиты информации от утечки по технически каналам в соответствии с техническим проектом и инструкциями по эксплуатации.

Уметь: оформлять рабочую и эксплуатационную документацию на средства и системы инженерно-технической защиты информации объекта информатизации; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы инженерно-технической защиты информации.

Владеть: навыками разработки технического проекта систем инженерно-технической защиты информации, акта обследования объекта защиты; навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации.

По дисциплине предусмотрена промежуточная аттестация в форме *зачёта с оценкой*.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлена основная литература*	23.03.2023	***8***

Приложение 1
к листу изменений

Обновление основной литературы (2023 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:
1. Дополнить раздел **Основная литература**

Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1900721

Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657

Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912992

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364

Составитель:
Кандидат технических наук,
и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин