



Государственное бюджетное образовательное учреждение высшего образования
Московской области

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

«УТВЕРЖДАЮ»

Проректор по
учебно-методической работе

Н.В. Бабина
«12» апреля 2022 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б.1.В.ДВ.03.03 «ПОДГОТОВКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ К
АТТЕСТАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(ООО «НОВО», ООО «ЦБИ»)»**

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

Королев
2022

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

Автор: Журавлев С.И. Рабочая программа дисциплины: «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО», ООО «ЦБИ»)». – Королев МО: «Технологический университет», 2022.

Рецензент: Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета.

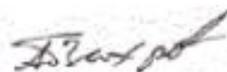
Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переподтверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№ 9 от 12.04.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО



к.т.н., доцент Вухров А.П.

Рабочая программа рекомендована на заседании УМС:

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

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

Целями изучения дисциплины является формирование у студентов базовых знаний и практических навыков в области проведения аттестации объектов информатизации по требованиям безопасности информации.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

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

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации

Основными **задачами** дисциплины являются:

1. Формирование у студентов базовых знаний в области аттестации объектов информатизации по требованиям безопасности информации, проведению специального обследования (СО), специальных проверок (СП) и специальных исследований, проводимых в ходе аттестации;

2. Ознакомление с основными нормативно-правовыми и методическими документами в области проведения специальных исследований и аттестации объектов информатизации по требованиям безопасности информации;

3. Привитие навыков практической работы с контрольно-измерительной аппаратурой, применяемой для аттестации объектов информатизации;

4. Привитие навыков разработки организационно-распорядительных документов, оформляемых по результатам аттестации объектов информатизации.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

Необходимые умения:

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;

Трудовые действия:

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО», ООО «ЦБИ»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

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

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очной формы составляет 3 зачетных единиц, 108 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 5	Семестр 7	Семестр ...	Семестр ...
Общая трудоемкость	108	108	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)		-			
Самостоятельная работа	66	66			
Другие виды контактной работы	10	10			
Практическая подготовка	16	16			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2 ч.	T1;T2	T1;T2			
Вид итогового контроля	Экзамен	Экзамен			

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очно	Практические занятия, час. Очно	Занятия в интерактивной форме, час. Очно	Практическая подготовка, час	Код компетенций
Раздел I. Обеспечение безопасного допуска к информационным ресурсам					
Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и	0.5	1	0.5		ПК-1

содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература					
Тема 2. Функции, состав, структура и задачи государственной системы защиты информации	0.5	1	0.5		ПК-1
Тема 3. Нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации	0.5	1	0.5		ПК-1
Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ (СЗИ) и проведение аттестации объектов информатизации	0.5	1	0.5		ПК-1
Тема 5. Основные положения законодательства в области защиты информации	0.5	1	0.5		ПК-1
Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе	0.5	1	0.5		ПК-1
Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации	0.5	1	0.5		ПК-1
Тема 8. Проведение аттестация объектов информатизации (ОИ)	0.5	1	0.5		ПК-1
Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации	1	1	1	2	ПК-2
Тема 10. Этапы практического проведения работ по	1	1	1	2	ПК-2

аттестации объектов информатизации					
Тема 11. Проверка и испытание аттестуемого объекта информатизации	1	1	0.5	2	ПК-2
Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам	1	1	0.5	2	ПК-2
Тема 13. Пассивные и активные методы защиты объектов информатизации	2	1	0.5	2	ПК-2
Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	2	1	0.5	2	ПК-2
Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа	2	1	0.5	2	ПК-2
Тема 16. Методики оценки защищённости объектов информатизации	2	1	0.5	2	ПК-2
Итого:	162	166	120	16	

4.2. Содержание тем дисциплины

Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература

Значение, предмет изучения и краткое содержание курса «Аттестация объектов информации». Место дисциплины среди других курсов, изучаемых студентами. Методы изучения дисциплины. Названия тем, распределение их по видам аудиторных занятий. Форма проверки знаний. Научная, учебная и периодическая литература по дисциплине. Знания, умения и компетенции, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных понятий по аттестации объектов информации применительно к изучению курса. Нормативно-методические

документы, регулирующие вопросы аттестации объектов информатизации.

Тема 2. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).

Что такое ГСЗИ, ее функции, состав, структура и задачи.

Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

Функции федерального органа по сертификации и аттестации.

Функции органов по аттестации.

Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации

Содержание Положения о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27.10.1995 № 199.

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

Содержание Положения об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание Типового положения об испытательной лаборатории, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание руководящих документов Гостехкомиссии России в области аттестации объектов информатизации. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К). Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.

Основное содержание Требований к системам обнаружения вторжений, утверждённых приказом ФСТЭК России от 06.12.2011 № 638.

Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утверждённого приказом ФСТЭК России от 15.03.2012 № 27. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).

Содержание Порядка проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Содержание национальных стандартов в области аттестации объектов информатизации.

Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ и проведение аттестации объектов информатизации

Содержание Федерального закона от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности».

Содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации". Содержание Приказ ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"

Содержание Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

Тема 5. Основные положения законодательства в области защиты информации

Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности». Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации». Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Основное содержание

Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.

Выполняемые работы на предпроектной стадии по обследованию объекта информатизации; содержание аналитического обоснования необходимости создания системы защиты информации; содержание технического задания на разработку системы защиты информации; содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)

Основные требования и рекомендации по защите речевой КИ.

Защита КИ, циркулирующей с системах звукоусиления и звукового сопровождения.

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

Тема 8. Проведение аттестация объектов информатизации (ОИ)

Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.

Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации

Перечень работ по подготовке объекта информатизации к аттестации.

Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.

Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

Тема 10. Этапы практического проведения работ по аттестации объектов информатизации

Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.

Последовательность проведения работ по аттестации защищаемых помещений.

Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.

Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

Тема 11. Проверка и испытание аттестуемого объекта информатизации

Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам

Содержание работ по поставке средств защиты информации от утечки по техническим каналам.

Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

Тема 13. Пассивные и активные методы защиты объектов информатизации

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.

Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке

Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа

Общие требования и рекомендации по защите информации (ЗИ) в автоматизированных системах (АС). Основные требования и рекомендации по ЗИ.

Методика формирования комплекса мероприятий по защите информационных систем в условиях возможного воздействия злоумышленников.

Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.

Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

Тема 16. Методики оценки защищённости объектов информатизации

Методика оценки защищённости помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

Методика оценки защищённости ОТСС от утечки конфиденциальной информации (КИ) за счёт наводок на токоведущие коммуникации.

Временная методика оценки защищённости помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО», ООО «ЦБИ»)» приведена в Приложении 1.

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

Основная литература:

1. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book03198> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

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

3. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book71525> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

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

Дополнительная литература:

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

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал;
2. <http://informika.ru/> – образовательный портал;
3. www.wiklsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи;
4. www.biblioclub.ru - Универсальная библиотека онлайн;
5. www.rucont.ru - ЭБС «Руконт»;
6. <http://www.academy.it.ru/> – академия АЙТИ;
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации;
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации;
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю;
11. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации;
12. <http://www.gov.ru> - Официальный сервер органов государственной власти Российской Федерации;
13. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;
14. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю.

9. Методические указания для обучающихся, по освоению дисциплины

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

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

Перечень программного обеспечения: MSOffice.

Информационные справочные системы:

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

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курс «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО», ООО «ЦБИ»)»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

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**

**«ПОДГОТОВКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ К АТТЕСТАЦИИ ПО
ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(ООО «НОВО», ООО«ЦБИ»»**

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

Королев
2022

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Требуемые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способность проводить исследования защищенности и информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1-16	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:1-16	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности и по совершенствованию системы ЗИ;	- применять действующую нормативную базу выбирать целесообразные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;

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

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
ПК-1,2	<i>Доклад</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> <i>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p> 	<p><i>Например: Проводится в письменной и/или устной форме.</i></p> <p><i>Критерии оценки:</i></p> <ol style="list-style-type: none"> <i>1. Соответствие содержания доклада заявленной тематике (1 балл).</i> <i>2. Качество источников и их количество при подготовке работы (1 балл).</i> <i>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</i> <i>4. Качество самой представленной работы (1 балл).</i> <i>5. Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл).</i> <p><i>Максимальная сумма баллов - 5 баллов.</i></p>
ПК-1,2	<i>Выполнение контрольной работы</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u></i> 	<p><i>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</i></p>

		<p><i>уровне – 4 балла;</i></p> <ul style="list-style-type: none"> • <i>компетенция освоена на базовом уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция не сформирована) – 2 и менее баллов</i></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. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

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

Формой контроля знаний по дисциплине « Аттестация в области защиты информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>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%.</i>
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	ПК-1,2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<i>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%.</i>
<i>Проводится в</i>	Зачет	ПК-1,2	3 вопроса	Зачет	Результат	Критерии

<p><i>сроки, установленные графиком образовательного процесса</i></p>				<p>проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.</p>	<p>ы предоставляются в день проведения зачета</p>	<p>оценки: «Зачтено»: 1. знание лексического и грамматического материала; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях в течение семестра; 4. ответ на вопросы зачета. «Не зачтено»: 1. демонстрирует частичные знания по темам дисциплин; 2. незнание лексического и грамматического материала; 3. неумение использовать и применять полученные знания; 4. не работал на практических занятиях; 5. не отвечает на вопросы зачета.</p>
<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>Экзамен</p>	<p>ПК-1,2</p>	<p>3 вопроса</p>	<p>Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.</p>	<p>Результаты предоставляются в день проведения экзамена</p>	<p>Критерии оценки: «Отлично»: <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на </p>

						<p>практике;</p> <ul style="list-style-type: none"> • работа на практически х занятиях; • знание основных научных теорий, изучаемых предметов; • 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
--	--	--	--	--	--	---

					<p>и применять полученные знания на практике;</p> <ul style="list-style-type: none"> • не работал на практических занятиях; <p>«Неудовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.
--	--	--	--	--	--

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации РКІ.
9. Компоненты и сервисы инфраструктуры открытых ключей.

10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

Тестовые задания для контроля остаточных знаний

1. Что понимается под аттестацией объектов информатизации?
 - контрольная проверка объекта информатизации, по результатам которой выдается сертификат соответствия требованиям по безопасности информации;
 - оснащение объекта информатизации средствами защиты, по результатам которой выписывается паспорт или паспорт соответствия требованиям по безопасности информации;
 - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - аттестата соответствия подтверждается, что объект соответствует требованиям стандартов;
 - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - лицензии подтверждается, что объект соответствует требованиям стандартов.
2. Какие объекты информатизации подлежат обязательной аттестации?
 - объекты информатизации, предназначенные для обработки конфиденциальной информации в коммерческих организациях;
 - объекты информатизации, предназначенные для обработки конфиденциальной информации в бюро кредитных историй;
 - объекты информатизации, предназначенные для обработки информации, составляющие государственную тайну, управления экологически опасными объектами, ведения секретных переговоров ;
 - объекты информатизации, предназначенные для обработки информации, составляющей коммерческую тайну.

3. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?

- технический паспорт объекта информатизации;
- матрицу доступа к объекту вычислительной техники, аттестованному по требованиям безопасности информации;
- протоколы испытаний и заключение по результатам проведения специальных исследований объекта информатизации;
- аттестат соответствия объекта информатизации требованиям по безопасности информации.

4. Какие классы защищенности от несанкционированного доступа реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации?

- 1А, 1Б, 1В;
- 2А, 3А;
- 2Б, 3Б;
- 1Г, 1Д.

5. Когда проводят испытания несертифицированной продукции, используемой на объекте информатизации, подлежащем обязательной аттестации?

- в ходе проведения аттестационных испытаний объекта информатизации;
- после предварительного ознакомления с объектом аттестации;
- после оформления, регистрации и выдачи аттестата соответствия;
- до подачи и рассмотрения заявки на аттестацию объекта информатизации.

1.2. Типовые вопросы, выносимые на экзамен

1. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).

2. Основные нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации.

3. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации защищаемых помещений по требованиям безопасности информации.

4. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

5. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

6. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

7. Последовательность проведения работ по аттестации защищаемых помещений.

8. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации объектов вычислительной техники по требованиям безопасности информации.

9. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

10. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?

11. Перечислить и пояснить классы защищенности от несанкционированного доступа, которые реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации.

12. Порядок проведения аттестации объекта информатизации.

13. Перечень и содержание документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

14. Перечень и содержание документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

15. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

16. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

17. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

18. Документы, оформляемые и разрабатываемые при проверках и испытаниях аттестуемого объекта информатизации в процессе его эксплуатации.

19. Основные положения методики оценки защищенности помещения, аттестованного по требованиям безопасности конфиденциальной информации; оценка защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

20. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищенности помещения, аттестованного по требованиям безопасности конфиденциальной информации.

21. Основные положения методики оценки защищенности объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.

22. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищенности объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

23. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).

24. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.

25. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.
26. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К).
27. Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.
28. Основное содержание Требования к системам обнаружения вторжений, утвержденных приказом ФСТЭК России от 06.12.2011 № 638.
29. Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утвержденного приказом ФСТЭК России от 15.03.2012 № 27.
30. Основное содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).
31. Основное содержание Порядка проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.
32. Основное содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
33. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.
34. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации".
35. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации".
36. Основное содержание ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
37. Основное содержание ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования

**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.*

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

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

**«ПОДГОТОВКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ К АТТЕСТАЦИИ ПО
ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(ООО «НОВО», ООО «ЦБИ»)»**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Безопасность телекоммуникационных систем

(в аэрокосмической сфере)

Уровень высшего образования: бакалавр

Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является формирование у студентов базовых знаний и практических навыков в области проведения аттестации объектов информатизации по требованиям безопасности информации.

Задачами дисциплины являются:

1. формирование у студентов базовых знаний в области аттестации объектов информатизации по требованиям безопасности информации, проведению специального обследования (СО), специальных проверок (СП) и специальных исследований, проводимых в ходе аттестации;
2. ознакомление с основными нормативно-правовыми и методическими документами в области проведения специальных исследований и аттестации объектов информатизации по требованиям безопасности информации;
3. привитие навыков практической работы с контрольно-измерительной аппаратурой, применяемой для аттестации объектов информатизации;
4. привитие навыков разработки организационно-распорядительных документов, оформляемых по результатам аттестации объектов информатизации.

2. Указания по проведению практических занятий

Тема 1- 2. Введение. Функции, состав, структура и задачи государственной системы защиты информации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Функции государственной системы защиты информации в соответствии с основными правовыми и нормативно методическими документами.

2. Состав, структура и задачи государственной системы защиты информации в соответствии с основными правовыми и нормативно-методическими документами.

Продолжительность занятия: 1 ч.

Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 2.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

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

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Положение о сертификации средств защиты информации по требованиям безопасности информации.
2. Руководящие документы Гостехкомиссии России, используемые при аттестации объектов информатизации, и их содержание.
3. Основное содержание национальных стандартов в области аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств защиты информации (СЗИ) и проведение аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 3.

Вид практического занятия: **подготовка доклада.**

Образовательные технологии: **групповая дискуссия.**

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

- базовые протоколы криптографической защиты информации.

- квантовая криптография.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).
2. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.
3. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 5. Основные положения законодательства в области защиты информации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 4.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки управления ключами.

Основные положения темы занятия:

- Управление ключами.
- Взаимодействие с УЦ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Конституция РФ, федеральные законы, Указы Президента РФ, постановления и распоряжения Правительства РФ об информационной безопасности общества и его граждан.
2. Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности».
3. Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Основное содержание Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

6. Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Продолжительность занятия: 1 ч.

Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе

Вид практического занятия: занятие в смешанной форме

Практическое занятие 5.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.
2. Выполняемые работы на предпроектной стадии по обследованию объекта информатизации;
3. Содержание аналитического обоснования необходимости создания системы защиты информации;
4. Содержание технического задания на разработку системы защиты информации;
5. Содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

Продолжительность занятия: 1 ч.

Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)

Вид практического занятия: занятие в смешанной форме

Практическое занятие 6.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

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

Продолжительность занятия: 1 ч.

Тема 8. Проведение аттестация объектов информатизации (ОИ)

Вид практического занятия: занятие в смешанной форме

Практическое занятие 7.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.
2. Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

Продолжительность занятия: 1 ч.

Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 8.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Перечень работ по подготовке объекта информатизации к аттестации.
2. Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.
3. Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.
3. Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

Продолжительность занятия: 1 ч.

Тема 10. Этапы практического проведения работ по аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 9.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.
2. Последовательность проведения работ по аттестации защищаемых помещений.
3. Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.
4. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

Продолжительность занятия: 1 ч.

Тема 11. Проверка и испытание аттестуемого (аттестованного) объекта информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 10.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

2. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

3. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

Продолжительность занятия: 1 ч.

Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам

Вид практического занятия: занятие в смешанной форме

Практическое занятие 11.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Содержание работ по поставке средств защиты информации от утечки по техническим каналам.

2. Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

Продолжительность занятия: 1 ч.

Тема 13. Пассивные и активные методы защиты объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 12.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.

2. Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

Продолжительность занятия: 1.5 ч.

Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке

Вид практического занятия: занятие в смешанной форме

Практическое занятие 13.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
2. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.
3. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Продолжительность занятия: 1.5 ч.

Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа

Вид практического занятия: занятие в смешанной форме

Практическое занятие 14.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.
2. Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

Продолжительность занятия: 1.5 ч.

Тема 16. Методики оценки защищённости объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 15.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы

1. Методика оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание; оценка защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.
2. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации.

3. Методика оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.

4. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

Продолжительность занятия: 2.5 ч.

3. Указания по проведению лабораторных работ

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Тема 13. Пассивные и активные методы защиты объектов информатизации	<p><i>Подготовка докладов по темам:</i></p> <ol style="list-style-type: none"> 1. Место информационной безопасности в системе национальной безопасности. 2. Современная концепция информационной безопасности. 3. Цели и концептуальные основы защиты информации. 4. Критерии, условия и принципы отнесения информации к защищаемой. 5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 6. Понятие и структура угроз защищаемой информации. 7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. 8. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
2.	Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	<p><i>Подготовка докладов по темам:</i></p> <ol style="list-style-type: none"> 1. Виды уязвимости информации и формы ее проявления. 2. Каналы и методы несанкционированного доступа к конфиденциальной информации. 3. Модель нарушителя. 4. Модель угроз. 5. Критерии оценки безопасности информационных технологий.

		<p>6. Методы защиты информации от несанкционированного доступа.</p> <p>7. Риски информационной безопасности.</p>
3	<p>Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа</p>	<p>Подготовка докладов по темам:</p> <ol style="list-style-type: none"> 1. Вредоносные программы и антивирусные программные средства. 2. Методы программно-аппаратной защиты информации. 3. Аттестация объектов информатизации. 19. Виды защиты информации. 4. Системы защиты информации. 5. Модели разграничения доступа. 6. Криптографические стандарты и их использование в информационных системах. 7. Способы и средства защиты информации от утечки по техническим каналам. 8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
4	<p>Тема 16. Методики оценки защищённости объектов информатизации</p>	<p>Подготовка докладов по темам:</p> <ol style="list-style-type: none"> 1. Основные нормативные правовые акты в области информационной безопасности и защиты информации. 2. Отечественные и зарубежные стандарты в области компьютерной безопасности. 3. Принципы и методы организационной защиты информации. 4. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях. 5. Лицензирование и сертификация в области защиты информации. 6. Комплексные системы защиты информации.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым

устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

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

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объем контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
5. Компьютерная преступность в экономических областях.
6. Мир XXI века: информационное противоборство.
7. Компьютерные вирусы в современных информационных системах.
8. Информационные угрозы современным экономическим объектам.
9. Информатизация России и проблема защиты информации.
10. Безопасность информации в коммерческой деятельности.
11. Разведки России – исторический аспект.
12. Мировой информационный терроризм.
13. Этика защиты информации.
14. Становление и развитие промышленного шпионажа.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book03198> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2. Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/256274> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3. Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

<https://e.lanbook.com/book71525> (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

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

Дополнительная литература:

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

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.wiklsec.ru - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. <http://www.academy.it.ru/> - академия АЙТИ.
7. <http://www.minfin.ru/> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю
11. <http://www.minfin.ru> - официальный сайт Министерства финансов Российской Федерации.
12. <http://www.gov.ru> - сервер органов государственной власти Российской Федерации.

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

Электронные ресурсы образовательной среды Университета

Информационно-справочные системы (Консультант+; Гарант).
Рабочая программа и методическое обеспечение по курсу «Подготовка
объекта информатизации к аттестации по требованиям безопасности
информации (ООО «НОВО», ООО «ЦБИ»)».