



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

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

«__» _____ 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б.1.В.ДВ.08.04 «РАЗРАБОТКА И СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ И ТЕХНИЧЕСКИХ СРЕДСТВ
В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ (ООО «ЦБИ»»**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев

2023

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

Автор: Рыженко С.В. Рабочая программа дисциплины: «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО «ЦБИ»)». – Королев МО: «Технологический университет», 2023.

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 11.04.2023 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)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО



Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

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:

Профессиональные компетенции:

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

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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:

- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;
- документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

Необходимые умения:

- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;
- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);
- участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;

Трудовые действия:

- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ).

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении 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», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для 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 очно-заочной формы составляет 2 зачетных единиц, 72 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 8	Семестр 9	Семестр ...	Семестр ...
Общая трудоемкость	72	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	36	36			
Лекции (Л)	12	12			
Практические занятия (ПЗ)	24	24			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	28	28			
Практическая подготовка	12	12			
Другие виды контактной работы	6	6			
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	Зачет	Зачет			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	20		20		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	12		12		
Лабораторные работы (ЛР)	-		-		
Самостоятельная работа	52		52		
Практическая подготовка	4		4		
Другие виды контактной работы	6		6		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+ -		+ -		
Вид итогового контроля	Зачет		Зачет		

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

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очно/заочное	Практические занятия, час. Очно/заочное	Занятия в интерактивной форме, час. Очно/заочное	Практическая подготовка, час	Код компетенций
Тема 1. Перечень документов и работ по подготовке объекта информатизации к аттестации	1/1	3/1	1/2	2/0.5	ПК-2
Тема 2. Этапы практического проведения работ по аттестации объектов информатизации	1/1	3/1	1/2	2/0.5	ПК-2
Тема 3. Проверка и испытание аттестуемого объекта информатизации	1/1	3/1	1/2	2/0.5	ПК-4
Тема 4. Поставка и установка средств защиты информации от утечки по техническим каналам	1/1	3/1	1/2	2/0.5	ПК-4
Тема 5. Пассивные и активные методы защиты объектов информатизации	2/1	3/	2/2	2/-	ПК-5
Тема 6. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	2/1	3/2	2/2	2/-	ПК-5
Тема 7. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа	2/1	3/2	2/2	3/1	ПК-5
Тема 8. Методики оценки защищённости объектов информатизации	2/1	3/2	2/2	3/1	ПК-2,4,5
Итого:	12/8	24/12	18/12	18/4	

4.2. Содержание тем дисциплины

Тема 1. 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 2. 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 3. 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 4. 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 5. 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 6. 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 7. 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 8. Методики оценки защищённости объектов информатизации

Методика оценки защищенности 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 «Разработка объекта информатизации в защищенном исполнении (ОАО «НОВО»)» 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/book/103198> (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/book/171525> (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.wikisec.ru - Энциклопедия информационной безопасности. –

Публикации, статьи;

4. www.biblioclub.ru - Универсальная библиотека онлайн;
5. www.rucont.ru - ЭБС «Рукопт»;
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:**
Электронные ресурсы образовательной среды Университета.
Информационно-справочная система (Консультант+;Гарант).

Ресурсы информационно-образовательной среды Университета:
Рабочая программа и методическое обеспечение по курсу «Разработка объекта информатизации в защищенном исполнении (ООО «НОВО»)

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**

**«РАЗРАБОТКА И СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ И ТЕХНИЧЕСКИХ СРЕДСТВ В ЗАЩИЩЕННОМ
ИСПОЛНЕНИИ ООО «ЦБИ»»**

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает::		
				Требуемые действия	Необходимые умения	Необходимые знания
1.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:1,2,3,4	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;	- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы организации по проведению экспериментальной деятельности в области ЗИ;
2.	ПК-4	Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении и внештатных ситуаций	Тема 1-16	- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств	- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);	- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

				защиты информации ;		
3.	ПК-5	Способность ю проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений	Темы 1-16	- анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)	- участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;	- документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

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-2,4,5	Тест	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов; • компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов; <p>В) не сформирована (компетенция <u>не сформирована</u>) – менее 50% правильных ответов</p>	<p>Например: Проводится письменно. Время, отведенное на процедуру - 30 минут. Неявка – 0 баллов. Критерии оценки определяются процентным соотношением. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.</p>
ПК-2,4,5	Доклад	<p>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом</u> уровне – 4 балла; • компетенция освоена на <u>базовом</u> уровне – 3 балла; <p>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</p>	<p>Например: Проводится в письменной и/или устной форме. Критерии оценки:</p> <ol style="list-style-type: none"> 1. Соответствие содержания доклада заявленной тематике (1 балл). 2. Качество источников и их количество при подготовке работы (1 балл). 3. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4. Качество самой

			<p>представленной работы (1 балл).</p> <p>5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p>
ПК-2,4,5	<p>Выполнение контрольной работы</p>	<p>А) полностью сформирована (компетенция освоена на <u>высоком уровне</u>) – 5 баллов</p> <p>Б) частично сформирована:</p> <ul style="list-style-type: none"> • компетенция освоена на <u>продвинутом уровне</u> – 4 балла; • компетенция освоена на <u>базовом уровне</u> – 3 балла; <p>В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов</p>	<p>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</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 «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении ООО «ЦБИ»» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Недел я текущ его контр оля	Вид оценочного средства	Код компетен ций, оцениваю щий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
	тестирован ие	ПК-2,4,5	20 вопросов	Компьютерн ое тестировани е ; время отведенное на процедуру - 30 минут	Результат ы тестирован ия предоставл яются в день проведения процедуры	<i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворител ьно – менее 50% правильных ответов Удовлетворительн о - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</i>

	тестирование	ПК-2,4,5	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>
	Зачет	ПК-2,4,5	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии 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.
--	--	--	--	--

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

Вопрос 1. Какой вариант наиболее полно представляет базовые технологии безопасности информации в ОС?

Вопрос 2. Какие из перечисленных подсистем должна включать система защиты информации?

Вопрос 3. Какие методы используются для затруднения подбора пароля к похищенному ключевому носителю?

Вопрос 4. В каком варианте перечислены атаки, специфичные для ОС?

Вопрос 5. Укажите номера основных характеристик качества ОС.

Вопрос 6. В каком варианте полно перечислены документы, представляющие основные решения по реализации политики безопасности предприятия?

Вопрос 7. В каком варианте перечислены характерные черты в области стратегий обеспечений безопасности информационных ресурсов организации?

Вопрос 8. В каком варианте дано наиболее точное определение понятий добровольного и принудительного управления доступом?

Вопрос 9. Перечислите номера методов аутентификации, характерных для ОС.

Вопрос 15. В каком варианте правильно указаны причины проведения аудита ОС?

Вопрос 16. Какой вариант наиболее полно представляет базовые технологии безопасности информации в СУБД предприятия?

Вопрос 17. Какие из перечисленных подсистем должна включать система защиты информации?

Вопрос 18. Какие методы используются для затруднения подбора пароля к похищенному ключевому носителю?

Вопрос 19. В каком варианте перечислены атаки, специфичные для баз данных?

Вопрос 20. Укажите номера основных характеристик качества систем баз данных.

Вопрос 21. В каком варианте наиболее полно сформулировано понятие динамического ограничения целостности базы данных?

Вопрос 22. Какими привилегиями должен обладать пользователь, создающий таблицу с первичным ключом?

Вопрос 23. В каком варианте правильно перечислены функциональные блоки системы разграничения доступа базы данных? Вставьте номера функциональных блоков в структурную схему диспетчера доступа.

Вопрос 24. В каком варианте полно перечислены документы, представляющие основные решения по реализации политики безопасности предприятия?

Вопрос 25. В каком варианте перечислены характерные черты в области стратегий обеспечений безопасности информационных ресурсов организации?

Вопрос 26. В каком варианте дано наиболее точное определение понятий добровольного и принудительного управления доступом?

Вопрос 27. Перечислите номера методов аутентификации, характерных для СУБД Oracle.

Вопрос 28. Какими привилегиями должен обладать пользователь, создающий таблицу в БД с внешним ключом?

Вопрос 29. Для каких целей необходим анализ включающей инфраструктуры сервера БД?

Вопрос 30. В каком варианте правильно указаны причины проведения аудита СУБД?

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.

Типовые вопросы, выносимые на зачет

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 Требований 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

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

**«РАЗРАБОТКА И СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ И ТЕХНИЧЕСКИХ СРЕДСТВ В ЗАЩИЩЕННОМ
ИСПОЛНЕНИИ ООО «ЦБИ»»**

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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. Перечень документов и работ по подготовке объекта информатизации к аттестации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

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

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.

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

Продолжительность занятия: 3/2 ч.

Тема 2. Этапы практического проведения работ по аттестации объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 2

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

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

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: 3/2 ч.

Тема 3. Проверка и испытание аттестуемого (аттестованного) объекта информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 3.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

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

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: 3/2 ч.

Тема 4. Поставка и установка средств защиты информации от утечки по техническим каналам

Вид практического занятия: занятие в смешанной форме

Практическое занятие 4.

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: 3/2 ч.

Тема 5. Пассивные и активные методы защиты объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 5.

Вид практического занятия: *подготовка доклада*.

Образовательные технологии: *групповая дискуссия*.

Тема и содержание практического занятия:

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

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: 3/2 ч.

Тема 6. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке

Вид практического занятия: занятие в смешанной форме

Практическое занятие 6

Вид практического занятия: *подготовка доклада*.

Образовательные технологии: *групповая дискуссия*.

Тема и содержание практического занятия:

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

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: 3/2 ч.

Тема 7. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа

Вид практического занятия: занятие в смешанной форме

Практическое занятие 7.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

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

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: 3/2 ч.

Тема 8. Методики оценки защищённости объектов информатизации

Вид практического занятия: занятие в смешанной форме

Практическое занятие 8

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: 3/2 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 5. Пассивные и активные методы защиты объектов информатизации	<p>Подготовка докладов по темам:</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. 9. Виды уязвимости информации и формы ее проявления. 10. Каналы и методы несанкционированного доступа к конфиденциальной информации.
2.	Тема 6. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке	<p>Подготовка докладов по темам:</p> <ol style="list-style-type: none"> 1. Модель нарушителя. 2. Модель угроз. 3. Критерии оценки безопасности информационных технологий. 4. Методы защиты информации от несанкционированного доступа. 5. Риски информационной безопасности.
3	Тема 7. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа	<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.

		<p>5. Модели разграничения доступа.</p> <p>6. Криптографические стандарты и их использование в информационных системах.</p> <p>7. Способы и средства защиты информации от утечки по техническим каналам.</p> <p>8. Принципы организации информационных систем в соответствии с требованиями по защите информации.</p>
4	<p>Тема 8. Методики оценки защищённости объектов информатизации</p>	<p>Подготовка докладов по темам:</p> <p>1. Основные нормативные правовые акты в области информационной безопасности и защиты информации.</p> <p>2. Отечественные и зарубежные стандарты в области компьютерной безопасности.</p> <p>3. Принципы и методы организационной защиты информации.</p> <p>4. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.</p> <p>5. Лицензирование и сертификация в области защиты информации.</p> <p>6. Комплексные системы защиты информации.</p>

5. Указания по проведению контрольных работ

5.1. Требования к структуре

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

5.2. Требования к содержанию (основной части)

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

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

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

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

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

5.3. Требования к оформлению

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

5.4. Примерная тематика контрольных работ:

1. Сформулируйте преимущества и недостатки использования технологии шифрования данных с явным заданием ключа.
2. Сформулируйте понятие статического ограничения целостности баз данных.
3. Сформулируйте понятие ссылочной целостности баз данных.
4. Сформулируйте понятие динамического ограничения целостности баз данных. Каким образом реализуются динамические ограничения целостности баз данных?
5. Сформулируйте понятие транзакции.
6. Опишите существо действия «фиксация транзакции».
7. Сформулируйте понятие уровня изоляции. Какие уровни изоляции поддерживает сервер баз данных Oracle.
8. Опишите типы блокировок и ситуации, когда для защиты БД целесообразно использовать каждый тип блокировок.
9. Обоснуйте необходимость анализа включающей инфраструктуры для оценки уровня защищенности баз данных.
10. Какая служба ОС Windows реализует работу прослушивающего процесса для сервера баз данных Oracle.
11. Какая служба ОС Windows реализует работу экземпляра сервера баз данных Oracle.
12. Обоснуйте целесообразность проведения аудита безопасности систем баз данных.
13. Опишите вариант управления событиями, фиксируемыми средствами аудита, с использованием конфигурационного файла. Назовите СУБД, в которой используется такой подход.
14. Опишите процесс активации средств аудита в СУБД Oracle.
15. С какой целью могут использоваться средства избирательного аудита в СУБД?
16. Опишите область применения специальных процедур, запускаемых средствами избирательного аудита в СУБД.

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/book/103198> (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/book/171525> (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-справочная система (Консультант+; Гарант).

Рабочая программа и методическое обеспечение по курсу «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении ООО «ЦБИ»»