МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор-
проректор по ОД
И.Г. Гайрабеков
«26» 06 2026г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ»

Направление подготовки

10.03.01 *«Информационная безопасность»*

Направленность (профиль)

«*Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*»

Квалификация

Бакалавр

Год начала подготовки – 2026

Грозный – 2026

1. Цели и задачи дисциплины

Целью освоения дисциплины «Комплексное обеспечение защиты информации объекта информатизации» (КОЗИОИ) является формирование у обучаемых знаний в области теоретических и практических основ построения комплексной системы защиты информации (КСЗИ) объекта информатизации.

Задачи дисциплины:

- формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ организации, процесса функционирования и надежности комплексной информационной безопасности автоматизированной и компьютерной систем объекта информатизации;

– изучение основ построения и принципов управления КСЗИ автоматизированной системы (АС) и компьютерной системы (КС) объекта информатизации, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Анализ и оценка рисков информационной безопасности» относится к Блоку 1 Части, формируемой участниками образовательных отношений учебного плана. Для изучения курса требуется освоение следующих дисциплин: «Информатика», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

В свою очередь, данный курс, помимо самостоятельного значения, является дисциплиной, завершающей учебный курс, предшествующей дипломному проектированию.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ОП	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине (ЗУВ)**
Общепрофессиональные		
0ПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,	**ОПК-10.1.** Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности. **ОПК-10.2.** Уметь: в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение	**знать:** - основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности. **уметь:** - в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение

управлять процессом их реализации на объекте защиты	комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты. **ОПК-10.3.** Владеть: методами формирования и выполнения комплекса мер по информационной безопасности.	комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; **владеть:** - методами формирования и выполнения комплекса мер по информационной безопасности;
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	**ОПК-2.1.1.** Знать: возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб. **ОПК-2.1.2.** Уметь: проводить анализ функционального процесса объекта защиты и его информационных составляющих. **ОПК-2.1.3.** Владеть: методами анализа функционального процесса объекта защиты и его информационных составляющих.	**знать**: - возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб; **уметь**: - проводить анализ функционального процесса объекта защиты и его информационных составляющих; **владеть**: методами анализа функционального процесса объекта защиты и его информационных составляющих;
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;	**ОПК-2.3.1.** Знать: локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты **ОПК-2.3.2.** Уметь: разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты **ОПК-2.3.3**. Владеть: методами обеспечения безопасности объекта защиты	**Знать:** локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты; **Уметь:** разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты; **Владеть:** методами обеспечения безопасности объекта защиты.

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	Всего часов/ зач.ед.		Семестр	
	ОФО	ОЗФО	ОФО	ОЗФО
			8	8
Контактная работа	**48/1,33**	**64/1,8**	**48/1,33**	**64/1,8**
В том числе:				
Лекции	24/0,66	32/0,9	24/0,66	32/0,9
Лабораторные работы (ЛР)	24/0,66	32/0,9	24/0,66	32/0,9
Самостоятельная работа (всего)	**120/3,3**	**80/2,2**	**120/3,3**	**80/2,2**
В том числе:				
Расчетно-графические работы				
Темы для самостоятельного изучения	64/1,7	30/0,8	64/1,7	30/0,8
Подготовка презентаций	36/1	30/0,8	36/1	30/0,8
И(или) другие виды самостоятельной работы:				
Подготовка к лабораторным работам	-	-	-	-
Подготовка к зачету				
Подготовка к экзамену	20/0,6	20/0,6	20/0,6	20/0,6
Контроль	**12/0,33**	**36/1**	**12/0,33**	**36/1**
Вид отчетности	**экз.**	**экз.**	**экз.**	**экз.**
Общая трудоемкость дисциплины Час.	**180**	**180**	**180**	**180**
Зач. ед.	**5**	**5**	**5**	**5**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины	Лекц.		Лаб. зан.		Всего часов/з.е.	
		ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
8 семестр							
1	Принципы организации и разработки комплексной системы защиты информации (КСЗИ) объекта информатизации	2	6	2	6	4	12
2	Потенциальные каналы и методы НСД к информации. Условия функционирования КСЗИ	4	6	4	6	8	12

3	Материально-техническое и нормативно-методическое обеспечение КСЗИ	8	8	8	8	16	16
4	Принципы и методы планирования функционирования КСЗИ	6	6	6	6	12	12
5	Подходы к оценке эффективности КСЗИ	4	6	4	6	8	12

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
8 семестр		
1.	Принципы организации и разработки комплексной системы защиты информации (КСЗИ) объекта информатизации	Методологические основы КОЗИОИ. Основные положения теории систем. Источники, причины, обстоятельства и условия дестабилизирующего воздействия на информацию. Выявления способов воздействия на информацию. Ущерб от потенциального дестабилизирующего воздействия на информацию. Оценка источников, способов и результатов дестабилизирующего воздействия на информацию
2.	Потенциальные каналы и методы НСД к информации. Условия функционирования КСЗИ	Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования защиты. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.
3.	Материально-техническое и нормативно-методическое обеспечение КСЗИ	Материально-техническое обеспечение функционирования КСЗИ. Нормативно-методические документы по обеспечению функционирования КСЗИ. Нормативно-методические документы в зависимости от вида объекта информатизации. Основные нормативнометодические документы организации по ЗИ.
4.	Принципы и методы планирования	Понятие и задачи планирования функционирования КОЗИОИ. Способы и стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов организации и функционирования КОЗИОИ.

	функционирования КСЗИ	Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов.
5.	Подходы к оценке эффективности КСЗИ	Оценка эффективности систем. Вероятностный подход: структуризация предметной области оценки, анализ. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям. Содержание и особенности экспертной оценки эффективности защиты. Классификационная структура методов и моделей оценки. Системы показателей защищенности (эффективности). Области применения и анализ приемлемости различных методов и моделей для оценки эффективности.

5.3. Лабораторный практикум

Таблица 5

№ п/п	**Наименование раздела**	**Наименование лабораторных работ**
8 семестр		
1.	Принципы организации и разработки комплексной системы защиты информации (КСЗИ) объекта информатизации	**Лабораторная работа №1.** Моделирование работы емкостного средства обнаружения нарушителей, расположенного внутри объекта информатизации
2.	Потенциальные каналы и методы НСД к информации. Условия функционирования КСЗИ	**Лабораторная работа №2.** Моделирование работы однопозиционного допплеровского радиолучевого средства обнаружения
3.	Материально-техническое и нормативно-методическое обеспечение КСЗИ	**Лабораторная работа №3.** Моделирование работы инфракрасного средства обнаружения нарушителей.
4.	Принципы и методы планирования функционирования КСЗИ	**Лабораторная работа №4.** Организация консалтинговой компании
5.	Подходы к оценке эффективности КСЗИ	**Лабораторная работа №5.** Оценка эффективности защиты информации важных объектов.

5.4. Практические занятия (семинары) – не предусмотрены.

6. Самостоятельная работа

6.1. Тематика и формы самостоятельной работы студентов

Таблица 6

№№ п/п	**Тематика докладов с презентациями**
1	Основные понятия области защиты информации (ЗИ) и информационной

	безопасности (ИБ): угроза, риск, инцидент, ущерб. Различия в понимании ЗИ и ИБ. Отличия системы от совокупности подсистем или элементов (синергетичность).
2	Материальные расходы на ЗИ, их рациональная область. Функциональная и экономическая эффективности системы защиты информации, существующие критерии. Минимизация ущерба.
3	Показатели качества защищаемой информации. Цели и задачи системы комплексной защиты информации (СКЗИ). Разноплановые методы защиты информации – административные, правовые, организационные, технические, программные.
4	Сценарии нарушения СКЗИ. Нарушители (злоумышленники) СКЗИ, их основные типы и соответствующее описание. Защита от внутреннего и внешнего нарушителя.
5	Основные параметры по оценке функциональной эффективности технических устройств ЗИ – вероятность обнаружения и вероятность ложной тревоги (наработка на ложную тревогу). Ошибки первого и второго рода.
6	СЗИ как автоматизированная организационно-техническая система, роль человека. Нечеткие (недетерминированные) методы исследования СФЗ. Комплексный характер защиты информации.
7	Принципы построения технической защиты информации. Природные способы защиты. Многозональность защиты информации. Назначение и типовые рубежи (зоны) защиты.
8	Подсистемы комплексной системы защиты информации (КСЗИ) – краткое описание, взаимосвязь. Преимущества интегрирования различных подсистем ЗИ в единую суперсистему. Идеальная система защиты информации.
9	Система (подсистема) физической защиты информации (СФЗ) как часть КСЗИ – цель функционирования, основные решаемые задачи и общий состав.
10	Категории объектов защиты (охраны). Задачи физической защиты информации. Профилактика в системе защиты. Задержка источника угроз, реакции на угрозу.
11	Система (подсистема) охранной сигнализации в составе СФЗ – цель, основные задачи и тактико-технические параметры. Физические принципы обнаружения нарушителей. Полезные сигналы и помехи.
12	Шкала длин волн электромагнитного излучения и ее использование в СФЗ. Видимый диапазон – основные особенности. ИК и УФ-диапазоны длин волн электромагнитного излучения.
13	Комплексирование средств обнаружения. Основные логические схемы и выражения для оценки сигнализационной надежности. Средняя наработка на ложную тревогу.
14	Система (подсистема) контроля и управления доступа в составе СФЗ – цель, основные задачи. Идентификация и аутентификация. Основные методы 10 аутентификации личности, их характеристики.
15	Система (подсистема) охранного телевидения в составе СФЗ – цель, основные задачи. Видеоаналитика, известные алгоритмы видео-обнаружения и видеоидентификации. Моделирование видеоканала извлечения видеоинформации.
16	Обнаружение, распознавание, идентификация цели в системах цифрового фото- и видео- наблюдения. Преимущества и недостатки цифровых и пленочных фотоаппаратов. Условия, влияющие на качество видеонаблюдения. Низкоуровневые телевизионные камеры. Устройства ночного видения. Тепловизоры.

17	Система (подсистема) сбора и обработки информации в составе СФЗ – цель, основные задачи. Вспомогательные системы в составе СФЗ. Автоматизированные рабочие места по управлению системой.
18	Технические каналы утечки информации. Простые и составные каналы утечки, их основные показатели. Характеристики источников и приемников сигналов технических каналов утечки, сред распространения.
19	Система (подсистема) защиты от утечки и перехвата информации по 4-м типам технических (физических) каналов, как часть КСЗИ. Акустический канал утечки информации, основные параметры и возможности средств добывания информации. Типы акустоэлектрических преобразователей. Микрофоны, их характеристики, классификация закладных устройств.
20	Угрозы, создаваемые случайными акустоэлектрическими преобразователями. Средства лазерного подслушивания. Средства высокочастотного навязывания. Основные методы противодействия подслушиванию: зашумление, экранировка.
21	Оптический канал утечки информации – основные параметры источников, среды распространения. Возможности средств добывания информации. Средства радиолокационного наблюдения с летательных и космических аппаратов.
22	Методы противодействия подглядыванию, оценка дальности видимости. Оптические волокна. Подслушивающие устройства телефонных линий. Способы добывания информации из оптического волокна. Эффективность маскировки, виды маскировочного окрашивания. Засветка и ослепление.
23	Источники побочных низкочастотных и высокочастотных излучений. Распространение электромагнитных волн. Опасные случайные и функциональные сигналы. Виды побочных электромагнитных излучений и наводок (ПЭМИН). Опасные сигналы в цепях электропитания, утечка информации по цепям заземления.
24	Радиоэлектронные каналы утечки информации, среды распространения сигналов. Особенности распространения радиоволн различных диапазонов. Способы повышения их дальности. Помехи в радиоэлектронном канале утечки.
25	Комплексы перехвата радиосигналов. Особенности сканирующих радиоприемников, способы определения координат источников радиоизлучений.
26	Вещественный канал утечки информации. Методы гарантированного физического и компьютерного уничтожения носителей информации. Преимущества и недостатки космической разведки.
27	Признаки наличия закладных устройств. Методы поиска и локализации радиоизлучающих и неизлучающих закладных устройств. Поиск проводных телефонных закладных устройств. «Чистка» помещений от закладок. Нелинейные радиолокаторы.
28	Система (подсистема) технического закрытия (сокрытия) информации в составе КСЗИ. Техническое закрытие речевой информации в телефонных каналах. Частотные и временные скремблеры. Вокодеры.
29	Система (подсистема) криптографической защиты информации в составе КСЗИ. Шифрование - основной метод защиты информации в радиоканалах связи. Типы кодируемых сообщений.
30	Система (подсистема) сетевой и антивирусной защиты компьютерной информации в рамках КСЗИ. Антивирусы. Межсетевые экраны.

31	Система (подсистема) администрирования и контроля эффективности защиты информации в рамках КСЗИ. Методы контроля эффективности защиты информации.

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Капгер И.В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : Пермский национальный исследовательский политехнический университет, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/158850.html (дата обращения: 03.09.2026). — Режим доступа: для авторизир. пользователей.

2. Овчинникова Е.А. Основы управления информационной безопасностью : учебное пособие / Е. А. Овчинникова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2023. — 167 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/138782.html (дата обращения: 03.09.2026). — Режим доступа: для авторизир. пользователей.

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

Вопросы к 1ой рубежной аттестации:

1. Методологические основы КОЗИОИ. Основные положения теории систем.
2. Источники, причины, обстоятельства и условия дестабилизирующего воздействия на информацию. Выявления способов воздействия на информацию.
3. Ущерб от потенциального дестабилизирующего воздействия на информацию.
4. Оценка источников, способов и результатов дестабилизирующего воздействия на информацию
5. Факторы, влияющие на выбор компонентов КСЗИ.
6. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ.
7. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования защиты.
8. Обеспечение полноты составляющих защиты.
9. Учет всех факторов и обстоятельств, оказывающих влияние на качество.
10. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.
11. Материально-техническое обеспечение функционирования КСЗИ.
12. Нормативно-методические документы по обеспечению функционирования КСЗИ.
13. Нормативно-методические документы в зависимости от вида объекта информатизации.
14. Основные нормативнометодические документы организации по ЗИ.
15. Модели анализа риска.

Образец билета к1-ой рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Комплексное обеспечение защиты информации объекта информатизации»
1-я рубежная аттестация
Вариант 1

1. Методологические основы КОЗИОИ. Основные положения теории систем.
2. Обеспечение полноты составляющих защиты.

Преподаватель_____ _____ М.М. Намаева

Вопросы ко 2ой рубежной аттестации:

1. Понятие и задачи планирования функционирования КОЗИОИ.
2. Способы и стадии планирования.
3. Факторы, влияющие на выбор принципов и способов планирования.
4. Структура и общее содержание планов организации и функционирования КОЗИОИ.
5. Методы сбора, обработки и изучения информации, необходимой для планирования.
6. Организация выполнения планов.
7. Оценка эффективности систем.
8. Вероятностный подход: структуризация предметной области оценки, анализ.
9. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям.
10. Содержание и особенности экспертной оценки эффективности защиты.
11. Классификационная структура методов и моделей оценки.
12. Системы показателей защищенности (эффективности).
13. Области применения и анализ приемлемости различных методов и моделей для оценки эффективности.
14. Выбор методов и средств защиты информации на основе анализа рисков.

Образец билета к 2-ой рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Комплексное обеспечение защиты информации объекта информатизации»
2-я рубежная аттестация
Вариант 1

1. Организация выполнения планов.
2. Выбор методов и средств защиты информации на основе анализа рисков.

Преподаватель_____ _____

7.2. Вопросы к экзамену

1. Методологические основы КОЗИОИ. Основные положения теории систем.
2. Источники, причины, обстоятельства и условия дестабилизирующего воздействия на информацию. Выявления способов воздействия на информацию.
3. Ущерб от потенциального дестабилизирующего воздействия на информацию.
4. Оценка источников, способов и результатов дестабилизирующего воздействия на информацию
5. Факторы, влияющие на выбор компонентов КСЗИ.
6. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ.
7. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования защиты.
8. Обеспечение полноты составляющих защиты.
9. Учет всех факторов и обстоятельств, оказывающих влияние на качество.
10. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.
11. Материально-техническое обеспечение функционирования КСЗИ.
12. Нормативно-методические документы по обеспечению функционирования КСЗИ.
13. Нормативно-методические документы в зависимости от вида объекта информатизации.
14. Основные нормативнометодические документы организации по ЗИ.
15. Модели анализа риска.
16. Понятие и задачи планирования функционирования КОЗИОИ.
17. Способы и стадии планирования.
18. Факторы, влияющие на выбор принципов и способов планирования.
19. Структура и общее содержание планов организации и функционирования КОЗИОИ.
20. Методы сбора, обработки и изучения информации, необходимой для планирования.
21. Организация выполнения планов.
22. Оценка эффективности систем.
23. Вероятностный подход: структуризация предметной области оценки, анализ.
24. Подход на основе формирования требований к объекту: классы защищенности и их характеристики, контрольные процедуры, определение соответствия защиты установленным требованиям.
25. Содержание и особенности экспертной оценки эффективности защиты.
26. Классификационная структура методов и моделей оценки.
27. Системы показателей защищенности (эффективности).
28. Области применения и анализ приемлемости различных методов и моделей для оценки эффективности.
29. Выбор методов и средств защиты информации на основе анализа рисков.

Образец билета к экзамену:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации»
Группа: **Семестр:**

Билет 1

1. Факторы, влияющие на выбор компонентов КСЗИ.
2. Оценка эффективности систем.
3. Выбор методов и средств защиты информации на основе анализа рисков.

Преподаватель _____ **Зав.кафедрой** _____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий
Лабораторная работа №4. Организация консалтинговой компании

Цель работы: Познакомиться на практике с организационной структурой компании по проведению аудиту информационной безопасности предприятия.

Программно-аппаратные средства: компьютерная лаборатория, стандартные средства Microsoft Office.

Теоретическая часть:

Консалтинг — деятельность по консультированию производителей, продавцов, покупателей по широкому кругу вопросов в сфере технологической, технической, экспертной деятельности. Цель консалтинга — помочь менеджменту в достижении заявленных целей. Консалтинговые компании специализируются по отдельным направлениям деятельности (например, финансовом, организационном, стратегическом)

Основная задача консалтинга заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Информационная безопасность (ИБ) некоторой ИС – это уровень ее защищенности от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, изменения или разрушения их компонентов.

Система защиты информации (СЗИ) – это система, обеспечивающая информационную безопасность некоторой ИС.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности некоторой информационной системы, в соответствии с определенными критериями и показателями безопасности.

Конфиденциальность (Confidentiality of Information) – это свойство информации быть известной только допущенным пользователям ИС.

Целостность (Integrity of Information) – это свойство информации быть неизменной в семантическом отношении.

Доступность (Availability of Information) – это свойство информации быть свободной на доступ в определенный момент времени.

Доступ к информации (Access to Information) – возможность ознакомления с информацией, ее обработка. Например, чтение, копирование, модификация или уничтожение информации.

Целостность, конфиденциальность и доступность ресурсов ИС вполне возможно измерять, например, на качественных шкалах, привлекая экспертов.

Круг проблем, решаемых консалтингом, весьма широк, кроме того, специализация компаний, предоставляющих консалтинговые услуги, может быть различной: от узкой, ограничивающейся каким-либо одним направлением консалтинговых услуг (например, аудит), до самой широкой, охватывающей полный спектр услуг в этой области. Соответственно этому, каждый специалист (или каждая фирма), работающая в данной области, вкладываете понятие консалтинга собственный смысл и придает ему собственный оттенок, определяемый направлением деятельности конкретной компании.

Итак, Консалтинг - это вид интеллектуальной деятельности, основная задача которого заключается в анализе, обосновании перспектив развития и использования научно-технических и организационно-экономических инноваций с учетом предметной области и проблем клиента.

Консалтинг решает вопросы управленческой, экономической, финансовой, инвестиционной деятельности организаций, стратегического планирования, оптимизации общего функционирования компании, ведения бизнеса, исследования и прогнозирования рынков сбыта, движения цен и т.д. Иными словами, консалтинг - это любая помощь, оказываемая внешними консультантами, в решении той или иной проблемы.

Основная цель консалтинга заключается в улучшении качества руководства, повышении эффективности деятельности компании в целом и увеличении индивидуальной производительности труда каждого работника.

Согласно распространенному мнению, к услугам внешних консультантов обращаются в основном и в первую очередь те организации, которые оказались в критическом положении. Однако помощь в критических ситуациях - отнюдь не основная функция консалтинга.

Контрольные вопросы

1. Что такое консалтинг?
2. Какова основная задача консалтинга?
3. Что понимают под информационной безопасностью?
4. Что представляет собой система защиты информации?
5. Что понимают под аудитом ИБ?
6. Перечислите основные свойства информации.
7. Каковы способы измерения свойств информации?

Задание

1. Изучить основной теоретический материал
2. Создать структурную модель консалтинговой компании.
3. Провести организационные мероприятия по подготовке проведения аудита.
4. Уточнить цели и задачи аудита
5. Сформировать рабочую группу

6. Подготавливается и согласовывается техническое задание на проведение аудита компании (по вариантам).
7. Собирать информацию и дать оценку следующих мер и средств:

- организационных мер в области информационной безопасности;
- программно-технических средств защиты информации;
- обеспечения физической безопасности.

Отчет по лабораторной работе № 1

Название работы

Расчет рисков информационной безопасности.

Цель

Познакомиться на практике с методом расчета рисков ИБ на основе модели анализа угроз и уязвимостей от Digital Security.

Выполнил

Студент гр. № _____

ФИО _____

Отчет

1. Структура и описание консалтинговой компании.
2. Перечень услуг консалтинговой компании.
3. Состав рабочей группы:
4. Цели и задачи аудита ИБ:
5. Техническое задание:
6. Придумать или использовать реальную ИС некоторой организации (по вариантам).
7. Исходные данные о заказчике:
8. Выводы по результатам анализа исходных данных от заказчика
9. Ответы на контрольные вопросы:

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Таблица 7

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного средства**
	менее 41 баллов (неудовлетворите	**41-60 баллов (удовлетворитель**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
0ПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты					
знать: - основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: - в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: - методами формирования и выполнения комплекса мер по информационной безопасности;	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба					

знать: - возможные источники информационных угроз, их возможные цели, пути реализации и предполагаемый ущерб;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: - проводить анализ функционального процесса объекта защиты и его информационных составляющих; **владеть**: методами анализа функционального процесса объекта защиты и	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: методами анализа функционального процесса объекта защиты и его информационных составляющих;	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются	Успешное и систематическое применение навыков	
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;					
Знать: локальные нормативные акты, стандарты информационной безопасности и меры по обеспечению безопасности объекта защиты;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
Уметь: разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты;	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методами обеспечения безопасности объекта защиты.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- **для слепых:** задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или

надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

1. Капгер И.В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : Пермский национальный исследовательский политехнический университет, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/158850.html (дата обращения: 03.09.2026). — Режим доступа: для авторизир. пользователей.

2. Овчинникова Е.А. Основы управления информационной безопасностью : учебное пособие / Е. А. Овчинникова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2023. — 167 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/138782.html (дата обращения: 03.09.2026). — Режим доступа: для авторизир. пользователей.

10. Материально-техническое обеспечение дисциплины

10.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 3-07.

Аудитория 3-07, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

Методические указания по освоению дисциплины
«Комплексное обеспечение защиты информации объектов информатизации»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Обучение по дисциплине «Защита информации» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, доклады с презентациями, индивидуальная консультация с преподавателем).

Учебный материал структурирован и изучение дисциплины производится втематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10- 15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10-15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).
4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1-2 задачи.

2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям.

Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к лабораторным занятиям

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям, необходимо обратить особоевнимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение кконкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

1. Ответить на вопросы плана лабораторного занятия.
2. Выполнить домашнее задание.
3. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы

Цель организации самостоятельной работы по дисциплине «Защита информации» – это углубление и расширение знаний в области научной исследовательской деятельности; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоениясодержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к лабораторному занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. Лабораторноезанятие – это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнятьи задавать вопросы коллегам по обсуждению.

При подготовке к контрольной работе (рубежной аттестации) обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;

– в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов)

1. Доклад с презентацией
2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), лабораторных, к изданиям электронных библиотечных систем.

Разработчик:
Старший преподаватель кафедры
«Информатика и вычислительная техника» /З.А. Шудуева /

СОГЛАСОВАНО:
Зав.кафедрой «Информатика и
вычислительная техника» /_Э. Д. Алисултанова/

Директор ДУМР / М.А. Магомаева /