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
«22» 06 2025г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«АНАЛИЗ И ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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 – 2025

Грозный – 2025

1. Цели и задачи дисциплины

Целью дисциплины является формирование теоретических знаний и практических навыков исследований рисков в системах защиты информации у студентов профиля «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Задачи дисциплины:

-определить актуальность, основные цели и терминологию задач анализа рисков в системах информационной безопасности;

– изучить теоретические основы и модели анализа рисков;

- получить сведения об основных отечественных и международных стандартах по анализу рисков в системах защиты информации;

– освоить методологию и технологии анализа рисков при построении моделей угроз для объектов информатизации, возможных проблем и их решений, рассмотреть примеры разработки методик анализа рисков;

– ознакомиться с основами управления рисками в системах защиты информации.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Анализ и оценка рисков информационной безопасности» относится к Блоку 1 Обязательной части 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)**
Профессиональные		
ПК-1. Способен управлять защитой информации в автоматизированных системах	**ПК-1.1.** Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по	**знать:** - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам;

	техническим каналам; нормативные правовые акты в области защиты информации **ПК-1.2.** Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; **ПК-1.3.** Владеть: методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа	нормативные правовые акты в области защиты информации **уметь:** - определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; **владеть:** - методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа;
ПК-3. Способен осуществлять аудит защищенности информации в автоматизированных системах	**ПК-3.1.** Знать: методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам; принципы построения систем защиты информации; организационные меры по защите информации **ПК 3.2.** Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; применять инструментальные средства контроля защищенности информации в автоматизированных системах **ПК 3.3.** Владеть: методами оценки информационных рисков безопасности информации в автоматизированной системе.	**знать**: - методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам; принципы построения систем защиты информации; организационные меры по защите информации; **уметь**: - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; применять инструментальные средства контроля защищенности информации в автоматизированных системах; **владеть**: - методами оценки информационных рисков безопасности информации в автоматизированной системе;

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы		**Всего часов/ зач. ед.**		**Семестры**	
				8	**8**
		ОФО	**ОЗФО**	**ОФО**	**ОЗФО**
Контактная работа (всего)		**48/1,3**	**64/1,8**	**48/1,3**	**64/1,8**
В том числе:					
Лекции		24/0,6	32/0,9	24/0,6	32/0,9
Практические занятия		-	-	-	-
Семинары		-	-	-	-
Лабораторные работы		24/0,6	32/0,9	24/0,6	32/0,9
Самостоятельная работа (всего)		**156/4,3**	**116/3,2**	**156/4,3**	**116/3,2**
В том числе:					
Курсовая работа (проект)					
ИТР					
Рефераты		40/1,1	20/0,6	40/1,1	20/0,6
Работа над проектом		40/1,1	24/0,7	40/1,1	24/0,7
И (или) другие виды самостоятельной работы:					
Подготовка к лабораторным работам		40/1,1	36/1	40/1,1	36/1
Подготовка к практическим работам					
Подготовка к зачету					
Подготовка к экзамену		36/1	36/1	36/1	36/1
Контроль		**12/0,3**	**36/1**	**12/0,3**	**36/1**
Вид отчетности		**экзамен**	**экзамен**	**экзамен**	**экзамен**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**216**	**216**	**216**	**216**
	ВСЕГО в зач. единицах	**6**	**6**	**6**	**6**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	**Наименование раздела дисциплины по семестрам**	**Часы лекционных занятий**		**Часы лабораторных занятий**		**Всего часов**	
		ОФО	**ОЗФО**	**ОФО**	**ОЗФО**	**ОФО**	**ОЗФО**
1	Основные цели и терминология задач анализа рисков в системах информационной безопасности	4	6	4	6	8	12
2	Теоретические основы и модели анализа рисков	5	6	5	6	10	12

3	Стандарты по анализу рисков в системах ИБ	5	6	5	6	10	12
4	Задачи анализа рисков в системах ИБ	5	6	5	6	10	12
5	Основы управления рисками в системах защиты информации	5	8	5	8	10	16

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Основные цели и терминология задач анализа рисков в системах информационной безопасности	Понятие риска в различных сферах жизни общества. Взаимосвязь основных понятий в области оценки рисков. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска. Классификации и характеристики рисков.
2.	Теоретические основы и модели анализа рисков	Место анализа рисков в общей схеме управления ИБ. Подходы к оценке рисков ИБ: качественный, количественный. Экономическая модель оценки рисков. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации. Модели анализа риска.
3.	Стандарты по анализу рисков в системах ИБ	Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010. Методы оценки риска Характеристика отечественных документов по анализу уровня защищенности объектов информатизации. Характеристика зарубежных и международных стандартов. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.
4.	Задачи анализа рисков в системах ИБ	Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE. Документы ФСТЭК по оценке защищенности объектов информатизации.
5.	Основы управления рисками в системах защиты информации	Методики и ПО для оценки рисков ИБ. Метод анализа и управления рисками CRAMM. Методики и ПО для оценки рисков ИБ. Принятие решений по результатам оценки рисков. Политика обработки рисков. Подведение итогов. Основы минимизации рисков. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства. Выбор методов и средств защиты информации на основе анализа рисков.

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела	Наименование лабораторных работ
1.	Основные цели и терминология задач анализа рисков в системах информационной безопасности	**Лабораторная работа №1.** Организация консалтинговой компании
2.	Теоретические основы и модели анализа рисков	**Лабораторная работа №2.** Табличные методы оценки и анализа информационных рисков.
3.	Стандарты по анализу рисков в системах ИБ	**Лабораторная работа №3.** Расчет рисков информационной безопасности.
4.	Задачи анализа рисков в системах ИБ	**Лабораторная работа №4.** Инструментальные средства анализа и управления рисками.
5.	Основы управления рисками в системах защиты информации	**Лабораторная работа №5.** Разработка рекомендаций по информационной безопасности.

5.4. Практические (семинарские) занятия: нет

Таблица 6

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	**-**	**-**

6. Самостоятельная работа

Способ организации самостоятельной работы: подготовка проекта по заданной тематике, в соответствии таблицы 7

Таблица 7

№№ п/п	Тематика докладов с презентациями
1	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
2	ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности»
3	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3
4	ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

5	ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»
6	ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
7	ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»
8	ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности»
9	ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»
10	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
11	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
12	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
13	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
14	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
15	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
16	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
17	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями «Оранжевой книги».
18	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
19	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями «Оранжевой книги».

20	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями «Оранжевой книги».
21	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
22	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
23	Оценка защищенности ОС Windows XP Professional (NT, 2000) в соответствии со стандартами ISO.
24	Оценка защищенности ОС Linux в соответствии со стандартами ISO.
25	Сравнительный анализ антивирусных пакетов.

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, А. И. Толстой. — 3-е изд., перераб. и доп. — Москва : Горячая линия — Телеком, 2022. — 223 с. — (Вопросы управления информационной безопасностью ; кн. 2). — ISBN 978-5-9912-0962-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — Режим доступа: для авторизир. пользователей.

2. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — Режим доступа: для авторизир. пользователей.

3. Царегородцев А.В. Анализ рисков в процессах обеспечения информационной безопасности : монография / А. В. Царегородцев, С. В. Романовский, С. В. Волков. — Москва : ИНФРА-М, 2024. — ISBN 978-5-16-018719-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — Режим доступа: для авторизир. пользователей.

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

***Вопросы к первой рубежной аттестации*:**

1. Понятие риска в различных сферах жизни общества.
2. Взаимосвязь основных понятий в области оценки рисков.
3. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.
4. Классификации и характеристики рисков.

5. Место анализа рисков в общей схеме управления ИБ.
6. Подходы к оценке рисков ИБ: качественный, количественный.
7. Экономическая модель оценки рисков.
8. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации.
9. Модели анализа риска.

***Вопросы ко второй рубежной аттестации*:**

1. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010.
2. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010.
3. Методы оценки риска. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.
4. Характеристика зарубежных и международных стандартов.
5. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.
6. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005.
7. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ.
8. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков.
9. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.
10. Документы ФСТЭК по оценке защищенности объектов информатизации.
11. Методики и ПО для оценки рисков ИБ.
12. Метод анализа и управления рисками CRAMM.
13. Принятие решений по результатам оценки рисков.
14. Политика обработки рисков. Подведение итогов.
15. Основы минимизации рисков.
16. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.
17. Выбор методов и средств защиты информации на основе анализа рисков.

Образцы билетов рубежных аттестаций:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Анализ и оценка рисков информационной безопасности»
1-я рубежная аттестация
Группа: Семестр: 8
Билет №

1. Подходы к оценке рисков ИБ: качественный, количественный
2. Модели анализа риска

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Анализ и оценка рисков информационной безопасности»
2-я рубежная аттестация
Группа: Семестр: 8
Билет №

1. Политика обработки рисков. Подведение итогов
2. Принятие решений по результатам оценки рисков

Преподаватель_____

7.2. Вопросы к экзамену

ОФО 8 семестр, ОЗФО 8 семестр

1. Основные понятия защиты информации и информационной безопасности
2. Понятие риска в различных сферах жизни общества.
3. Взаимосвязь основных понятий в области оценки рисков.
4. Понятие киберриска, угрозы, уязвимости, понятие и виды ущерба от атак, тотальный и остаточный риск, качественный и количественный риск, предпринимательский риск, цели анализа риска.
5. Классификации и характеристики рисков.
6. Место анализа рисков в общей схеме управления ИБ.
7. Подходы к оценке рисков ИБ: качественный, количественный.
8. Экономическая модель оценки рисков.
9. Вероятностная модель оценки рисков основная концепция анализа рисков в системах защиты информации.
10. Модели анализа риска.
18. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010.
19. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010.
20. Методы оценки риска. Характеристика отечественных документов по анализу уровня защищенности объектов информатизации.
21. Характеристика зарубежных и международных стандартов.
22. Стандарты серии NIST SP 800, стандарты серии ISO/IEC, стандарт IEC 31010:2019.
23. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005.
24. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ.
25. Оценка, измерение и прогнозирование рисков. Характеристика современных методик анализа рисков.
26. Методики: ГРИФ, FRAP, RiskWatch, CRAMM, OCTAVE.
27. Документы ФСТЭК по оценке защищенности объектов информатизации.
28. Методики и ПО для оценки рисков ИБ.
29. Метод анализа и управления рисками CRAMM.
30. Принятие решений по результатам оценки рисков.
31. Политика обработки рисков. Подведение итогов.
32. Основы минимизации рисков.

33. Избегание рисков, передача и принятие рисков, страхование и диверсификация производства.
34. Выбор методов и средств защиты информации на основе анализа рисков.

Образец билета к экзамену:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Анализ и оценка рисков информационной безопасности»
Группа: Семестр: 8
Билет №

1. Методики и ПО для оценки рисков ИБ
2. Основы минимизации рисков
3. Политика обработки рисков. Подведение итогов

Подпись преподавателя_____ Подпись заведующего кафедрой _____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа №1. 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 8

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)**	
ПК-1. Способен управлять защитой информации в автоматизированных системах					
знать: **-** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам; нормативные правовые акты в области защиты информации;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: - определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации;	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: - методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

ПК-3. Способен осуществлять аудит защищенности информации в автоматизированных системах					
знать: - методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам; принципы построения систем защиты информации; организационные меры по защите информации;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; применять инструментальные средства контроля защищенности информации в автоматизированных системах;	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: - методами оценки информационных рисков безопасности информации в автоматизированной системе	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются	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. Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, А. И. Толстой. — 3-е изд., перераб. и доп. — Москва : Горячая линия — Телеком, 2022. — 223 с. — (Вопросы управления информационной безопасностью ; кн. 2). — ISBN 978-5-9912-0962-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — Режим доступа: для авторизир. пользователей.

2. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — Режим доступа: для авторизир. пользователей.

Царегородцев А.В. Анализ рисков в процессах обеспечения информационной безопасности : монография / А. В. Царегородцев, С. В. Романовский, С. В. Волков. — Москва : ИНФРА-М, 2024. — ISBN 978-5-16-018719-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 01.09.2026). — 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
«Анализ и оценка рисков информационной безопасности»

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 в тематической 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 особое внимание 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 к конкретной 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 освоения содержания 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. Лабораторное занятие – 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, уточнять и 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» / Х.М.Бапаева /

СОГЛАСОВАНО:

Зав.кафедрой «Информатика
и
вычислительная техника»
М.А. Магомаева /

Э. Д. Алисултанова/