МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	И.о. заведующего кафедрой информационных технологий
О.Н. Выборнова	О.Н. Выборнова
«5» мая 2025г.	«5» мая 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Анализ и оценка рисков

наименование

Составитель(-и)	**Выборнова О.Н., доцент, к.т.н, доцент кафедры ИТ**
Направление подготовки / специальность	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очно-заочная**
Год приема	**2023**
Курс	**4**
Семестр	**8**

Астрахань – 2025

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины «Анализ и оценка рисков» являются получение знаний о принципах построения систем информационной безопасности, методиках оценки рисков информационно безопасности, а также практических навыков применения средств анализа безопасности информационных систем.

1.2. Задачи освоения дисциплины (модуля):

- Изучить принципы построения современных систем информационной безопасности; принципы статистического анализа; способы описания поведения систем; типовые архитектуры и принципы построения современных защищенных информационных систем; угрозы и атаки, характерные для распределенных информационных систем.
- Сформировать умения формализовать задачу контроля параметров безопасности информационными системами; использовать нормативные правовые акты по анализу рисков в своей профессиональной деятельности; разрабатывать методы и средства для проверки выполнения требований информационной безопасности и поиска уязвимостей.
- Овладеть методиками оценки рисков информационной безопасности; средствами фиксации параметров безопасности информационных систем; методиками реализации и верификации моделей контроля и управления доступом; навыками применения средств анализа безопасности информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Анализ и оценка рисков» относится к части, формируемой участниками образовательных отношений, и осваивается в 8 семестре.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами*:*

- Информатика.
- Теория вероятностей и математическая статистика
- Организационное и правовое обеспечение информационной безопасности.
- Производственная практика

Знания: основных понятий информатики, структуры систем документационного обеспечения.

Умения: использовать программные и аппаратные средства персонального компьютера, пользоваться нормативными документами по защите информации.

Навыки: поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): методика и техника составления различных управленческих и иных документов учреждений, организаций и предприятий.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

Аттестация объектов информатизации.

Также дисциплина «Анализ и оценка рисков» поможет студентам при реализации задач преддипломной практики и написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) профессиональных (ПК):

ПК-1 – способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем.

ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	ПК-1.1. нормативные правовые акты в области защиты информации, организационные меры по защите информации, программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	ПК 1.2. определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения доступа, применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах	ПК-1.3. методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ПК 2.1. технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации	ПК 2.2. проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.	ПК 2.3. методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 3 зачетные единицы, в том числе 30 часов, выделенных на контактную работу обучающихся с преподавателем (из них 15 часов – лекции, 15 часов – лабораторные работы), и 78 часов – на самостоятельную работу обучающихся:

Таблица 2 – Структура и содержание дисциплины (модуля)

Раздел, тема дисциплины (модуля)	Семестр	Контактная работа (в часах)			Самост. работа		Формы текущего контроля успеваемости, форма промежуточной аттестации
		Л	ПЗ	ЛР	КР	СР	
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	8	1		1		10	Входное тестирование, проверка словаря терминов и определений, опрос на экзамене
Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.		2		2		8	Проверка решения задач, отчет по лабораторной работе, опрос на экзамене
Тема 3. Нормативно-правовые документы в области управления рисками. ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005. Вероятностная модель риска		2		2		8	Проверка решения задач, отчет по лабораторной работе, опрос на экзамене
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России		1		1		10	Контрольная работа №1, опрос на экзамене
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.		2		2		8	Отчет по лабораторной работе, опрос на экзамене
Тема 6. Методика CRAMM. Метод CORAS. Методика vsRisk.		2		2		8	Отчет по лабораторной работе, опрос на экзамене
Тема 7. Методика FRAP. Методика OCTAVE. Методика PTA		2		2		8	Отчет по лабораторной работе, опрос на экзамене
Тема 8. Методика RiskWatch. Методика компании Microsoft.		2		2		8	Отчет по лабораторной работе, контрольная работа №2, опрос на экзамене
Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.		1		1		10	Проверка обзора методик оценки рисков, опрос на экзамене
		15		**15**		**78**	**ЭКЗАМЕН**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК 1	ПК 2	
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	12	+	+	2
Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.	12	+	+	2
Тема 3. Нормативно-правовые документы в области управления рисками. ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005. Вероятностная модель риска	12	+	+	2
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России	12		+	1
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.	12	+	+	2
Тема 6. Методика CRAMM. Метод CORAS. Методика vsRisk.	12	+	+	2
Тема 7. Методика FRAP. Методика OCTAVE. Методика PTA	12	+	+	2
Тема 8. Методика RiskWatch. Методика компании Microsoft.	12	+	+	2
Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.	12	+	+	2
Итого	***108***			

Краткое содержание каждой темы дисциплины (модуля)

Тема 1

Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.

Тема 2

Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.

Тема 3

Нормативно-правовые документы в области управления рисками. ISO-15408:2002 «Общие критерии». ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005. Вероятностная модель риска.

Тема 4

Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России.

Тема 5
Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.

Тема 6
Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.

Тема 7
Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA.

Тема 8
Методики и программные продукты по управлению рисками. Методика RiskWatch. Методика компании Microsoft.

Тема 9
Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Лекционные занятия проводятся с демонстрацией тезисов материалов в виде презентации. При рассмотрении нормативно-правовых актов возможна демонстрация основных положений самого документа. Изложение материала практико-ориентированных разделов сопровождается примерами, позволяющими лучше усвоить материал.

На лабораторных занятиях преподаватель озвучивает цель и основные задачи лабораторной работы, комментирует ход выполнения работы и требования к отчету.

При подготовке к учебным занятиям необходимо воспользоваться учебно-методической литературой из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

При подготовке к учебным занятиям рекомендуется воспользоваться учебно-методической литературой из п.8, а также материалами, загруженными в ЭИОС.

В случае пропуска лекционного занятия необходимо ознакомиться с презентацией по теме в ЭИОС. При возникновении вопросов по содержимому лекции – обратиться за разъяснениями к преподавателю.

При подготовке к отчету лабораторной работы необходимо ответить на контрольные вопросы. Отчет осуществляется в виде демонстрации преподавателю хода выполнения работы, полученных результатов, а также ответа на контрольные вопросы. Допускается добавление ответов на контрольные вопросы в конец отчета по лабораторной работе.

В процессе изучения дисциплины обучающийся может использовать учебно-методические материалы на английском языке. Для этого необходимо обратиться к преподавателю.

Таблица 4 – Содержание самостоятельной работы обучающихся

Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Тема 1. Составление словаря терминов и определений	10	Внеаудиторная, участие студентов в составлении тестов, изучение учебных пособий

Тема 2. Решение задач. Ответы на контрольные вопросы к лабораторной работе	8	Внеаудиторная, изучение учебных пособий
Тема 3. ИСО 31010 Решение задач. Ответ на контрольные вопросы к лабораторной работе	8	Внеаудиторная, изучение учебных пособий
Тема 4. NIST SP800-30. ENISA. Выполнение контрольной работы	10	Внеаудиторная, изучение учебных пособий
Тема 5. Ответ на контрольные вопросы к лабораторной работе	8	Внеаудиторная, изучение учебных пособий
Тема 6. Метод CORAS. Ответ на контрольные вопросы к лабораторной работе	8	Внеаудиторная, изучение учебных пособий
Тема 7. Методика FRAP. Ответ на контрольные вопросы к лабораторной работе	8	Внеаудиторная, изучение учебных пособий
Тема 8. Ответ на контрольные вопросы к лабораторной работе Выполнение контрольной работы	8	Внеаудиторная, изучение учебных пособий
Тема 9. Политика обработки рисков.	10	Внеаудиторная, изучение учебных пособий составление обзора методик оценки рисков

В процессе изучения дисциплины обучающийся может использовать учебно-методические материалы на английском языке. Для этого необходимо обратиться к преподавателю.

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Словарь основных терминов и определений, касающихся риск-менеджмента – оформляется в печатном виде на листах формата А4 или в рукописном виде в тетради.

Обзор методик оценки рисков – оформляется в печатном виде на листах формата А4 или в рукописном виде в тетради. Содержит краткую информацию о рассмотренных в процессе обучения методиках оценки рисков: наименование, реализуемый метод (количественный, качественный, смешанный), этапы оценки, основные формулы и шкалы (при необходимости). Может быть оформлен в виде таблицы.

Отчет по лабораторной работе – оформляется и отчитывается в электронном виде: формат листа А4, книжная ориентация страницы. Отчеты по всем лабораторным работам имеют единый титульный лист, на котором указывается наименование дисциплины, ФИО и группа исполнителя, ФИО преподавателя, принимающего отчеты. В отчете по каждой лабораторной работе должно быть представлено наименование работы, цель, ход выполнения работы (скриншоты, краткое текстовое описание), выводы по результатам работы.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий, в том числе разбор конкретных ситуаций.

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	Обзорная лекция	Не предусмотрено	выполнение теста
Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Тема 3. Нормативно-правовые документы в области управления рисками. ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005. Вероятностная модель риска	Лекция	Не предусмотрено	выполнение лабораторной работы
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России	Лекция	Не предусмотрено	выполнение контрольной работы
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 6. Методика CRAMM. Метод CORAS. Методика vsRisk.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Тема 7. Методика FRAP. Методика OCTAVE. Методика PTA	Лекция	Не предусмотрено	выполнение контрольной работы, выполнение лабораторной работы
Тема 8. Методика RiskWatch. Методика компании Microsoft.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы

Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы

Отдельные лекционные и практические занятия могут проводиться на иностранном языке (английский язык).

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

– использование возможностей интернета в учебном процессе (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.);

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование виртуальной обучающей среды (LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 10 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
Microsoft Security Assessment Tool. Режим доступа: http://www.microsoft.com/ru-ru/download/details.aspx?id=12273 (Free) Windows Security Risk Management Guide Tools and	Программы для информационной безопасности

Templates. Режим доступа: http://www.microsoft.com/en-us/download/details.aspx?id=6232 (Free)	
Microsoft Visual Studio	Среда разработки
PyCharm EDU	Среда разработки

6.3.2. Современные профессиональные базы данных и информационные справочные системы:

1. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» http://dlib.eastview.com
2. Электронные версии периодических изданий, размещенные на сайте информационных ресурсов www.polpred.com
3. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информсистем»: https://library.asu-edu.ru/catalog/.
4. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/issledovaniya-i-innovacii/11745-nauchnye-jurnaly-agu.html.
5. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) http://mars.arbicon.ru
6. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине «Анализ и оценка рисков» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	ПК-1, ПК-2	Тест, практическое задание, вопросы к экзамену
Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.	ПК-1, ПК-2	Задачи, задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 3. Нормативно-правовые документы в области управления рисками. ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005. Вероятностная модель риска	ПК-1, ПК-2	задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30.	ПК-1, ПК-2	Вопросы контрольной работы №1, вопросы к экзамену

Оценка рисков ИБ – ENISA. Стандарт Банка России		
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.	ПК-1, ПК-2	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 6. Методика CRAMM. Метод CORAS. Методика vsRisk.	ПК-1, ПК-2	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 7. Методика FRAP. Методика OCTAVE. Методика PTA	ПК-1, ПК-2	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 8. Методика RiskWatch. Методика компании Microsoft.	ПК-1, ПК-2	Задание и вопросы к лабораторной работе, вопросы к контрольной работе №2, вопросы к экзамену
Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.	ПК-1, ПК-2	Практическое задание, вопросы к экзамену

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Для оценки результатов обучения применяются следующие критерии:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя

3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.

1. ***Входное тестирование*** (Примерные тестовые задания)

1. Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу и его несанкционированного использования
    a. Атака
    b. Актив
    c. Угроза
    d. Воздействие

2. Систематическое использование информации для выявления источников и оценки риска
    a. Атака
    b. Анализ риска
    c. Угроза
    d. Воздействие

3. Сочетание вероятности события и его последствий
    a. Риск
    b. Атака
    c. Актив
    d. Угроза

4. Возможная причина нежелательного инцидента, который может нанести ущерба системе или организации
    a. Атака
    b. Анализ
    c. Угроза
    d. Воздействие

5. Слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой
    a. Уязвимость
    b. Риск
    c. Атака
    d. Актив

2. Практическое задание «Словарь основных терминов и определений»

Изучить основные термины и определения в сфере риск-менеджера. Составить словарь (в тетради или на листах А4) с указанием ссылки на источник литературы.

Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.

1. Практическое задание (Решить задачу)

- Оцените ущерб, возникший вследствие атаки на защищаемый объект, при заданных данных: время простоя вследствие атаки – 2 часа, время восстановления после атаки – 8 часов, время повторного

ввода информации – 8 часов, зарплата обслуживающего персонала за месяц – 5 000 ден. ед., зарплата сотрудников атакованного узла – 6 000 ден. ед., количество обслуживающего персонала (администраторов) – 1, количество сотрудников атакованного узла – 4, объем продаж атакованного узла за год – 1 000 000 ден. ед., стоимость защиты обслуживания и запасных частей – 0 ден. ед., число атакованных узлов – 1, число атак в год – 5.

2. Лабораторная работа №1 «Экономическая модель оценки рисков»

ЗАДАНИЕ

Написать программу, реализующую экономическую модель оценки рисков.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Понятие уязвимости, угрозы, атаки, риска, оценки риска.
2. Экономическая модель оценки риска: основное содержание, достоинства, недостатки.

Тема 3. Нормативно-правовые документы в области управления рисками. ISO-15408:2002 «Общие критерии». ISO 31000 «Менеджмент риска». Методы управления рисками ИБ – ISO/IEC 27005:2011. Вероятностная модель риска

1. Практическое задание (Решить задачу)

- Оцените риск для услуги VPN, если: вероятность защищенности ПК 0,9. Вероятность защищенности пограничного маршрутизатора 0,999, вероятность защищенности межсетевого экрана 0,999. Основной угрозой для серверов (сервера политики, сервера сертификатов, сервера доступа) является угроза НСД. Меры и средства защиты от НСД представлены в таблице 2.1. При наличии охраны и пропускной системы первые 3 защитные меры преодолеваются с вероятностью 0,75. При использовании сменяемых паролей защитные меры 4, 5, 6 преодолеваются с вероятностью 0,3. При наличии криптографических средств защиты десятая защитная мера преодолевается с вероятностью 0,01. Защитные меры 7, 8, 9 не используются.

- Оцените величину риска для информационного актива, расположенного на персональном компьютере в кабинете учебного корпуса, предложенном преподавателем. Самостоятельно определить перечень мер и средств защиты от НСД на пути к данному активу и вероятности их преодоления (примерный перечень представлен в таблице).

2. Лабораторная работа №2 «Вероятностная модель оценки рисков»

ЗАДАНИЕ

Написать программу, реализующую вероятностную модель оценки рисков на примере атак на VPN. Для узлов VPN предусмотреть возможность задания вероятности защищенности или выбора мер защиты от НСД.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Модель риска типа «узла»: основное содержание, пример.
2. Вероятностная модель: основное содержание, достоинства, недостатки.
3. Отличие вероятностной модели оценки рисков от экономической модели оценки рисков.

Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарты Банка России

1. Контрольная работа № 1

1. Основные понятия: угроза, уязвимость, атака, риск, оценка риска.
2. Количественная оценка рисков. Достоинства, недостатки подхода.
3. Качественная оценка рисков. Достоинства, недостатки подхода.
4. Экономическая модель оценки рисков.
5. Вероятностная модель оценки рисков.
6. Классификация угроз информационной безопасности.
7. Этапы управления рисками.
8. Управление рисками и жизненный цикл информационной системы.
9. ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности». Понятия безопасности и их взаимосвязь.

10. Оценка рисков по ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности».
11. ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности». Профиль защиты.

Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.

1. ***Лабораторная работа №3 «Средство оценки рисков «Microsoft Security Assessment Tool» (MSAT)»***

   ЗАДАНИЕ

   1. Установить программное средство Microsoft Security Assessment Tool.
   2. Провести оценку рисков информационной безопасности выбранного предприятия с использованием программы Microsoft Security Assessment Tool.

   КОНТРОЛЬНЫЕ ВОПРОСЫ

   1. Понятие профиля риска для бизнеса.
   2. Концепция «эшелонированной защиты».
   3. Понятие уровня безопасности организации.

Тема 6. Методика CRAMM. Метод CORAS. Методика vsRisk.

1. ***Лабораторная работа №4 «Средство качественной оценки рисков vsRisk»***

   ЗАДАНИЕ

   1. Установить vsRisk.
   2. Провести оценку рисков информационной безопасности выбранного предприятия с использованием vsRisk.

   КОНТРОЛЬНЫЕ ВОПРОСЫ

   1. Методика оценки рисков, реализованная в программном продукте vsRisk.
   2. Этапы оценки рисков.
   3. Актив, типы активов.
   4. Риск, угроза, уязвимость, механизмы контроля.

Тема 7. Методика FRAP. Методика OCTAVE. Методика PTA

1. Лабораторная работа №5. Средство количественной оценки рисков Practical Threat Analysis

ЗАДАНИЕ

1. Установить программный продукт PTA.
2. Провести оценку рисков информационной безопасности выбранного предприятия с использованием программного продукта PTA.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Взаимосвязь понятий актив, угроза, уязвимость, контрмера в методике PTA.
2. Методика PTA: основные этапы.
3. Сравнение результатов количественной (PTA) и качественной (vsRisk) оценки рисков.

Тема 8. Методика RiskWatch. Методика компании Microsoft.

1. Лабораторная работа №6. Методика управления рисками Microsoft (The Security Risk Management Guide)

ЗАДАНИЕ

Провести оценку рисков информационной безопасности выбранного предприятия с использованием методики компании Microsoft.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Процесс управления рисками информационной безопасности, предлагаемый Microsoft: основные этапы.
2. Понятие уровня зрелости организации с точки зрения управления рисками безопасности.
3. Классы активов в методике Microsoft.

4. Качественная оценка рисков в методике Microsoft.
5. Количественная оценка рисков в методике Microsoft.

2. Контрольная работа №2

1. Метод CRAMM: цель разработки, концепция, общая схема метода.
2. Исследование системы ИБ методом CRAMM. Стадия 1: Идентификация ресурсов и построение модели ИС.
3. Исследование системы ИБ методом CRAMM. Стадия 2: Анализ угроз и уязвимостей
4. Исследование системы ИБ методом CRAMM. Стадия 3: Выбор контрмер. Достоинства и недостатки метода CRAMM.
5. Методика FRAP.
6. Метод OCTAVE: основные сведения, разработка профиля угрозы.
7. Метод OCTAVE: идентификация инфраструктурных уязвимостей.
8. Метод OCTAVE: разработка стратегии и планов безопасности.
9. Методика Risk Watch. Критерии управления рисками и их вычисление.
10. Методика Risk Watch. Этапы методики.
11. Метод CORAS.
12. Методика оценки рисков Microsoft Security Assessment Tools.
13. Методика оценки рисков компании Microsoft: классы активов, этап качественной оценки рисков.
14. Методика оценки рисков компании Microsoft: классы активов, этап количественной оценки рисков.
15. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Схема процесса менеджмента рисков. Установление контекста менеджмента риска.
16. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Критерии оценки, воздействия и принятия риска.
17. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Общее описание оценки рисков ИБ: идентификация активов, угроз, уязвимостей, средств защиты
18. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». методология измерения риска
19. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Обработка риска. Мониторинг и пересмотр, передача и принятие риска.
20. Методика Practical Threat Analysis.

Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.

1. Обзор методик оценки рисков

Оформить таблицу

Наименование методики оценки рисков	Реализуемый метод (количественный, качественный, смешанный)	Этапы оценки, основные формулы и шкалы

Перечень вопросов и заданий, выносимых на экзамен

1. Основные понятия: угроза, уязвимость, атака, риск, оценка риска.
2. Количественная оценка рисков. Достоинства, недостатки подхода.
3. Качественная оценка рисков. Достоинства, недостатки подхода.
4. Экономическая модель оценки рисков.
5. Вероятностная модель оценки рисков.
6. Классификация угроз информационной безопасности.
7. Этапы управления рисками.
8. Управление рисками и жизненный цикл информационной системы.
9. Метод CRAMM: цель разработки, концепция, общая схема метода.
10. Исследование системы ИБ методом CRAMM. Стадия 1: Идентификация ресурсов и построение модели ИС.
11. Исследование системы ИБ методом CRAMM. Стадия 2: Анализ угроз и уязвимостей

12. Исследование системы ИБ методом CRAMM. Стадия 3: Выбор контрмер. Достоинства и недостатки метода CRAMM.
13. Методика FRAP.
14. Метод OCTAVE: основные сведения, разработка профиля угрозы.
15. Метод OCTAVE: идентификация инфраструктурных уязвимостей.
16. Метод OCTAVE: разработка стратегии и планов безопасности.
17. Методика Risk Watch. Критерии управления рисками и их вычисление.
18. Методика Risk Watch. Этапы методики.
19. Метод CORAS.
20. Методика оценки рисков Microsoft Security Assessment Tools.
21. Методика оценки рисков компании Microsoft: классы активов, этап качественной оценки рисков.
22. Методика оценки рисков компании Microsoft: классы активов, этап количественной оценки рисков.
23. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Схема процесса менеджмента рисков. Установление контекста менеджмента риска.
24. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Критерии оценки, воздействия и принятия риска.
25. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Общее описание оценки рисков ИБ: идентификация активов, угроз, уязвимостей, средств защиты
26. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». методология измерения риска
27. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Обработка риска. Мониторинг и пересмотр, передача и принятие риска.
28. Стандарты Банка России по информационной безопасности.
29. Методика Practical Threat Analysis.
30. Методика vsRisk.
31. Методика R-Vision: Risk Manager
32. Принятие решений по результатам оценки рисков. Политика обработки рисков
33. Практические задания из тем 2 и 3.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем				
1.	Задание закрытого типа	В зависимости от возможной степени ущерба, наносимого организации в случае разглашения информации, применяются следующие степени конфиденциальности информации: 1. конфиденциально 2. строго конфиденциально 3. секретно 4. совершенно секретно	1, 2	2
2.		Сертификат соответствия – это	2	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		1. комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п 2. документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров 3. оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации		
3.		Сертификация – это 1. документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров 2. форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров 3. деятельность, заключающаяся в передаче или получении прав на проведение работ в	2	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		области защиты информации 4. степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты		
4.		Какая из перечисленных методик оценки рисков предполагает проведение серии семинаров, в рамках которых формируется представление об имеющихся рисках? 1. CRAMM 2. OCTAVE 3. MSAT 4. PTA	2	2
5.		Наиболее обобщенная совокупность требований доверия в соответствии со стандартом ИСО/МЭК 15408-3 называется 1. класс 2. семейство 3. компонент 4. сервис	1	2
6.	Задание открытого типа	Перечислите основные сервисы информационной безопасности	Основные сервисы информационной безопасности: доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно; – конфиденциальность – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя; – целостность – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.	8
7.		Перечислите основные стратегии приведения величины риска к приемлемому уровню	Снижение риска путем применения защитных мер, ликвидация источника угрозы, уклонение от угрозы, принятие риска и перенос ответственности на третье лицо (страхование)	5
8.		Опишите основные моменты, которые являются характерными для рисковой ситуации	Основные моменты, которые являются характерными для рисковой ситуации: случайный характер события, который определяет, какой из возможных исходов реализуется на практике; наличие альтернативных решений; известны вероятности исходов событий и ожидаемые результаты; существует вероятность возникновения убытков; существует вероятность получения дополнительной прибыли.	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
9.		По длительности во времени факторы риска подразделяются	По длительности во времени факторы риска подразделяются: 1) кратковременные – угроза потерь ограничена определенным отрезком времени; 2) постоянные – непрерывно угрожают предпринимательской деятельности в данном географическом районе или в определенной отрасли экономики	5
10.		По степени приемлемости факторы риска подразделяются	По степени приемлемости факторы риска подразделяются: 1) допустимый риск — угроза полной потери прибыли от реализации того или иного проекта или от предпринимательской деятельности в целом. 2) критический риск связан с опасностью потерь в размере произведенных затрат на осуществление данного вида предпринимательской деятельности или отдельной сделки. 3) катастрофический риск – угроза потерь в размере, равном или превышающем все имущественное состояние предпринимателя.	6
11.	Комбинированный	Необходимо выполнить оценку рисков в организации банковской сферы. Какой стандарт необходимо использовать? Почему? 1) ГОСТ ИСО 31000 2) СТО БР ИББС 3) CRAMM 4) ISO IEC 27005	2 Организации банковской сферы при оценке рисков должны руководствоваться стандартами Банка России	5
12.		Какой этап процесса управления рисками включает выявление источников угроз и оценку возможных воздействий на информационные активы? 1. Идентификация рисков 2. Анализ рисков 3. Реагирование на риски 4. Мониторинг рисков	1 Идентификация рисков — первый этап, включающий процесс выявления всех значимых угроз, уязвимостей и последствий, потенциально опасных для информационной среды	5
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации				
13.	*Задание закрытого типа*	Какие данные используются для количественной оценки риска? 1. Частота возникновения инцидента и возможный ущерб 2. Субъективные мнения экспертов 3. Истории прошлых инцидентов 4. Возможности улучшения инфраструктуры	1	2
14.		Риск, возникающий вследствие	1	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		политических, экономических факторов, связанный с резким изменением курса валюты 1. валютный 2. инфляционный 3. системный 4. общий		
15.		Независимая от реализации совокупность требований безопасности для некоторой категории объекта оценки, отвечающая специфическим запросам потребителя: 1. Профиль защиты 2. Линия защиты 3. Категория защиты 4. Информационная безопасность	1	3
16.		Экономическая модель позволяет оценить: 1. стоимость ущерба от реализации некоторой атаки 2. вероятность успешной атаки 3. эшелонирование средств защиты 4. информационный актив	1	3
17.		Вероятностная модель позволяет оценить: 1. стоимость ущерба от реализации некоторой атаки 2. вероятность успешной атаки 3. эшелонирование средств защиты 4. информационный актив	2	3
18.	*Задание открытого типа*	Задача: Оцените ущерб, возникший вследствие атаки на защищаемый объект, при заданных данных: время простоя вследствие атаки – 2 часа, время восстановления после атаки – 8 часов, время повторного ввода информации – 8 часов, зарплата обслуживающего персонала за месяц – 5 000 ден. ед., зарплата сотрудников атакованного узла –	Стоимость потерь: $П_{П} = \frac{\sum_{C=1}^{N_C} Z_C}{192} \cdot t_{П} = \frac{6000 \cdot 4}{192} \cdot 2 = 250 (ден.ед.)$ Стоимость повторного ввода информации: $П_{ВИ} = \frac{\sum_{C=1}^{N_C} Z_C}{192} \cdot t_{ВИ} = \frac{6000 \cdot 4}{192} \cdot 8 = 1000 (ден.ед.)$ Стоимость восстановления узла: $П_{ПВ} = \frac{\sum_{O=1}^{N_O} Z_O}{192} \cdot t_{В} = \frac{5000 \cdot 1}{192} \cdot 8 = 208{,}33 (ден.ед.)$ Стоимость восстановления работоспособности:	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		6 000 ден. ед., количество обслуживающего персонала (администраторов) – 1, количество сотрудников атакованного узла – 4, объем продаж атакованного узла за год – 1 000 000 ден. ед., стоимость защиты обслуживания и запасных частей – 0 ден. ед., число атакованных узлов – 1, число атак в год – 5.	$П_В = П_{ВИ} + П_{ПВ} + П_{ЗЧ} = 1000 + 208{,}33 + 0 = 1208{,}33 (ден.ед.)$ Выгода: $V = \frac{О_{ПР}}{52 \cdot 5 \cdot 8} \cdot (t_П + t_В + t_{ВИ}) = \frac{1000000 \cdot (2+8+8)}{2080} = 8653{,}85 (ден.ед.)$ Упущенная выгода: $U = П_П + П_В + V = 250 + 1208{,}33 + 8653{,}85 = 10112{,}18 (ден.ед)$ Общий ущерб от атаки: $О_у = \sum_n \sum_I U = 10112{,}18 \cdot 5 \cdot 1 = 50560{,}9 (ден.ед.)$ *Ответ:* Общий ущерб = 50 560,90 ден. ед.	
19.		Задача: Оцените риск для услуги VPN, если: вероятность защищенности ПК 0,9. Вероятность защищенности пограничного маршрутизатора 0,999, вероятность защищенности межсетевого экрана 0,999. Основной угрозой для серверов (сервера политики, сервера сертификатов, сервера доступа) является угроза НСД. Меры и средства защиты от НСД представлены в таблице 2.1. При наличии охраны и пропускной системы первые 3 защитные меры преодолеваются с вероятностью 0,75. При использовании сменяемых паролей защитные меры 4, 5, 6 преодолеваются с вероятностью 0,3. При наличии криптографических средств защиты десятая защитная мера преодолевается с вероятностью 0,01. Защитные меры 7, 8, 9 не используются.	Сначала необходимо вычислить вероятность сохранения защищенности серверов: $P_{СП} = P_{СД} = P_{СС} = P_i^{защ} = 1 - \prod_{r=1}^{N_i} P_{ir} =$ $= 1 - 0{,}75 \cdot 0{,}3 \cdot 0{,}01 = 0{,}998$ Далее подставляем полученные значения, а также значения вероятностей защищенности ПК, маршрутизатора и межсетевого экрана в формулу для нахождения вероятности успешной атаки: $P_{риск} = 1 - P_{ПК} \cdot P_{СД} \cdot P_{СП} \cdot P_{СС} \cdot P_{ПМ} \cdot P_{МЭ} \cdot P_П =$ $= 1 - 0{,}9 \cdot 0{,}998 \cdot 0{,}998 \cdot 0{,}998 \cdot 0{,}999 \cdot 0{,}999 \cdot 1 = 0{,}107$ *Ответ:* вероятность успешной атаки равна 0,107.	6
20.		Какие отчеты формируются в РТА, позволяющие получить более подробную информацию о проведенном анализе рисков, кроме обобщенного отчета (пункт меню Reports → All Reports)	Кроме обобщенного отчета в РТА формируются следующие отчеты, позволяющие получить более подробную информацию о проведенном анализе рисков (пункт меню Reports → All Reports): Аналитические отчеты: Эффективность контрмер; Планы по нейтрализации угроз; Оптимизированный план снижения рисков. Информационные отчеты: Детализированный перечень угроз; Детализированный перечень активов; Детализированный перечень уязвимостей;	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			Детализированный перечень контрмер; Наиболее опасные угрозы. Отчет самодиагностики: Полнота модели.	
21.		Для чего используется классификация активов при управлении рисками?	Классификация активов необходима для установления приоритета защитных мероприятий, исходя из важности конкретного ресурса для деятельности предприятия. Активы классифицируются по уровню критичности для бизнеса, влиянию на процессы и ценность данных	8
22.		Ситуационная задача: В организации имеют скудное представление о рисках, отсутствует статистика инцидентов нарушения информационной безопасности, мало исходных данных в числовом виде. Какую категорию методик оценки рисков следует выбрать в организации?	Необходимо выбрать качественную методику оценки рисков, потому что она подходит для начального анализа рисков. В таких методиках не требуются четкие числовые характеристики. Достаточно общего описания.	8
23.	*Комбинированный*	Почему аудит уязвимости является важным этапом управления рисками? Обоснуйте ответ. 1. Позволяет определить слабые места системы перед реальной атакой 2. Обеспечивает полное устранение всех существующих уязвимостей 3. Предупреждает возникновение внутренних угроз безопасности 4. Сокращает расходы на инфраструктуру безопасности	1 Аудит уязвимостей помогает выявить слабости информационных систем заранее, позволяя минимизировать последствия возможной атаки, поскольку выявленные проблемы могут быть устранены заблаговременно. Остальные пункты менее важны или вовсе неверны: полный контроль над всеми уязвимостями невозможен, внутренние угрозы требуют иных мер контроля, а сокращение расходов на безопасность редко достижимо таким образом	8
24.		Что такое регулярный мониторинг сети и почему он важен для снижения рисков? 1. Периодическое обновление программного обеспечения 2. Контроль изменений конфигурации сети 3. Постоянный сбор и анализ событий безопасности 4. Проведение ежегодных аудитов	3 Регулярный мониторинг сети заключается в постоянном наблюдении и сборе событий, связанных с безопасностью. Такой подход позволяет своевременно обнаружить возможные аномалии, предотвратить угрозу и оперативно реагировать на возникшие инциденты	7

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Фонд оценочных средств по дисциплине включает:
- вопросы к экзамену;
- набор вариантов контрольных работ и тестов;
- комплект заданий и контрольных вопросов к лабораторным работам.

Оценка качества освоения программы дисциплины включает текущий контроль успеваемости, промежуточную аттестацию, итоговую аттестацию.

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:
- небрежное выполнение,
- отсутствие выводов,
- нарушение сроков предоставления отчета.

Отчет не может быть принят и подлежит доработке в случае:
- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:
- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:
- даны два неверных ответа на теоретические вопросы.

Экзамен

Экзаменационный билет включает в себя 2 теоретических вопроса и 1 задачу.

Основаниями для снижения оценки являются:
- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- пересдача экзамена (1я – минус 5 баллов, 2я и последующие – минус 10 баллов).

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (50 баллов на семестровую часть: 40 баллов – текущие формы контроля и до 10 баллов – на бонусы; 50 баллов – на экзаменационную часть).

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения соответствующих работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На экзамене осуществляется комплексная проверка знаний, навыков и умений студентов по материалу дисциплины на основании ответов на теоретические вопросы и решения практических задач.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6/4	24	В соответствии с таблицей 2
2.	*Выполнение контрольной работы*	2/4	8	
3.	*Тест*	1/4	4	
4.	*Задача*	2/1	2	
5.	*Обзор методик*	1/2	2	
Всего			**40**	-
Блок бонусов				
6.	*Посещение занятий без пропусков*		3	
7.	*Своевременное выполнение всех заданий*		3	
8.	*Активность студента на занятии*		4	
Всего			**10**	-
Дополнительный блок				
9.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале
90–100	5 (отлично)
85–89	4 (хорошо)
75–84	
70–74	
65–69	3 (удовлетворительно)
60–64	
Ниже 60	2 (неудовлетворительно)

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература:

1. Бизнес-безопасность / И.Н. Кузнецов. - 4-е изд. - М. : Дашков и К, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785394026546.html ЭБС «Консультант студента»).
2. Системный подход к обеспечению информационной безопасности предприятия (фирмы) [Электронный ресурс] : Монография / Трайнев В.А. - 3-е изд. - М. : Дашков и К, 2020. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785394037504.html
3. Досмухамедов, Б. Р., Выборнова, О. Н., Ажмухамедов, И. М., Анализ рисков информационной безопасности : учебно-методическое пособие. Издательский дом «Астраханский университет», 2016. URL: https://biblio.asu-edu.ru/Reader/Book/2016100312360888500002063136 ЭБС Электронный Читальный зал – БиблиоТех).

8.2. Дополнительная литература:

1. Милославская Н.Г., Управление рисками информационной безопасности : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 2. - М. : Горячая линия - Телеком, 2013. - 130 с. (Серия "Вопросы управления информационной безопасностью") - ISBN 978-5-9912-0272-5 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202725.html
2. Математические основы теории риска [Электронный ресурс] : Учебн. пособ. / Королев В.Ю., Бенинг В.Е., Шоргин С.Я. - 2-е изд., перераб. и доп. - М. : ФИЗМАТЛИТ, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785922112673.html ЭБС «Консультант студента»).
3. Анализ и оценка риска производственной деятельности : Учеб. пособие / П.П. Кукин, В.Н. Шлыков, Н.Л. Пономарев, Н.И. Сердюк. - М. : Абрис, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785437200483.html (ЭБС «Консультант студента»).
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745747.html (ЭБС «Консультант студента»).
5. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А. - М. : ДМК Пресс, 2004. - (Информ. технологии для инженеров). - http://www.studentlibrary.ru/book/ISBN5940742467.html ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

2. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu-edu.ru/catalog/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).