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 ИБ
_____ Р.Ю. Демина	_____ Т.Г. Гурская
« 6 » июня 2024 г.	« 6 » июня 2024 г..

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Анализ и оценка рисков

наименование

Составитель(-и)	**Выборнова О.Н., к.т.н, доцент кафедры ИБ**
Направление подготовки / специальность	**09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ**
Направленность (профиль) ОПОП	**«Безопасность информационных систем»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очно-заочная**
Год приема	**2021**
Курс	**4**
Семестр	**8**

Астрахань – 2024

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.
- Математические основы информационных технологий и вычислительной техники
- 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):

Комплексное обеспечение защиты информации объекта 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-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности.	ПК-3.1. виды работ по созданию (модификации) и сопровождению информационных систем	ПК-3.2. выполнять работы по созданию, сопровождению, модификации и обеспечению информационной безопасности информационных систем.	ПК-3.3. Владеть навыками выполнения работ по созданию, сопровождению, модификации и обеспечению информационной безопасности информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 3 зачетные единицы, в том числе 54 часа, выделенных на контактную работу обучающихся с преподавателем (18 часов – лекции, 36 часов – лабораторные работы), и 54 часа – 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.	7	2		4		6	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		4		6	Проверка решения задач, отчет по лабораторной работе, опрос на экзамене
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		2		4		6	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		2		4		6	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		4		6	Отчет по лабораторной работе, опрос на экзамене
Тема 6. Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.		2		4		6	Отчет по лабораторной работе, опрос на экзамене
Тема 7. Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA		2		4		6	Отчет по лабораторной работе, опрос на экзамене
Тема 8. Методики и программные продукты по управлению рисками. Методика RiskWatch. Методика компании Microsoft.		2		4		6	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.		2		4		6	Проверка обзора методик оценки рисков, опрос на экзамене
		18		**36**		**54**	**ЗАЧЕТ**

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

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции	Общее количество компетенций
		ПК 3	
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	12	+	1
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	+	1
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	12	+	1
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	+	1
Тема 6. Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.	12	+	1

Тема 7. Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA	12	+	1
Тема 8. Методики и программные продукты по управлению рисками. Методика RiskWatch. Методика компании Microsoft.	12	+	1
Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.	12	+	1
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)

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8, а также ответить на контрольные вопросы из [1] по каждой лабораторной работе.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8, Интернет-источниками.

Таблица 4 – Содержание самостоятельной работы обучающихся

Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Тема 1. Информационная безопасность предприятия. Система защиты информации как экономического объекта. Существующие подходы по анализу и управлению ИБ.	6	Внеаудиторная, участие студентов в составлении тестов, изучение учебных пособий
Тема 2. Анализ и управление рисками. Основные понятия, задачи, цели. Преимущества данного подхода. Связь рисков с угрозами и уязвимостями ИБ предприятия. Экономическая модель риска.	6	Внеаудиторная, изучение учебных пособий
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	6	Внеаудиторная, изучение учебных пособий
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России	6	Внеаудиторная, изучение учебных пособий
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.	6	Внеаудиторная, изучение учебных пособий
Тема 6. Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.	6	Внеаудиторная, изучение учебных пособий
Тема 7. Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA	6	Внеаудиторная, изучение учебных пособий
Тема 8. Методики и программные продукты по управлению рисками. Методика RiskWatch. Методика компании Microsoft.	6	Внеаудиторная, изучение учебных пособий
Тема 9. Методики по управлению рисками, разработанные российскими специалистами и учеными. Принятие решений по результатам оценки рисков. Политика обработки рисков.	6	Внеаудиторная, изучение учебных пособий

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

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-15408:2002 «Общие критерии». 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	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы

рисков: количественные, качественные, смешанные методы. Методика MSAT.			
Тема 6. Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Тема 7. Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA	Лекция	Не предусмотрено	выполнение контрольной работы, выполнение лабораторной работы
Тема 8. Методики и программные продукты по управлению рисками. 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 материалов и заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.);

-использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы 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 (или системы управления обучением 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 Templates. Режим доступа: http://www.microsoft.com/en-us/download/details.aspx?id=6232 (Free)	Программы для информационной безопасности
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.
4. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
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

Контролируемые разделы, темы 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-3***	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-3***	Задачи, задание и вопросы к лабораторной работе, вопросы к экзамену
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	***ПК-3***	задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 4. Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. Стандарт Банка России	***ПК-3***	Вопросы контрольной работы №1, вопросы к экзамену
Тема 5. Этапы управления рисками. Интеграция управления рисками в жизненный цикл ИС. Основные подходы по оценке рисков: количественные, качественные, смешанные методы. Методика MSAT.	***ПК-3***	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 6. Методики и программные продукты по управлению рисками. Методика CRAMM. Метод CORAS. Методика vsRisk.	***ПК-3***	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 7. Методики и программные продукты по управлению рисками. Методика FRAP. Методика OCTAVE. Методика PTA	***ПК-3***	Задание и вопросы к лабораторной работе, вопросы к экзамену
Тема 8. Методики и программные продукты по управлению рисками. Методика RiskWatch. Методика компании Microsoft.	***ПК-3***	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-3***	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, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при 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. Методики и программные продукты по управлению рисками. 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. Методики и программные продукты по управлению рисками. 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. Методики и программные продукты по управлению рисками. 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 к зачету

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. Типы рисков по Паркеру и Бенсону.
8. Этапы управления рисками.
9. Управление рисками и жизненный цикл информационной системы.
10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности». Понятия безопасности и их взаимосвязь.
11. Оценка рисков по ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности».
12. ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности». Профиль защиты.
13. Метод CRAMM: цель разработки, концепция, общая схема метода.
14. Исследование системы ИБ методом CRAMM. Стадия 1: Идентификация ресурсов и построение модели ИС.
15. Исследование системы ИБ методом CRAMM. Стадия 2: Анализ угроз и уязвимостей
16. Исследование системы ИБ методом CRAMM. Стадия 3: Выбор контрмер. Достоинства и недостатки метода CRAMM.
17. Методика FRAP.
18. Метод OCTAVE: основные сведения, разработка профиля угрозы.
19. Метод OCTAVE: идентификация инфраструктурных уязвимостей.
20. Метод OCTAVE: разработка стратегии и планов безопасности.
21. Методика Risk Watch. Критерии управления рисками и их вычисление.
22. Методика Risk Watch. Этапы методики.
23. Метод CORAS.
24. Методика оценки рисков Microsoft Security Assessment Tools.
25. Методика оценки рисков компании Microsoft: классы активов, этап качественной оценки рисков.

26. Методика оценки рисков компании Microsoft: классы активов, этап количественной оценки рисков.
27. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Схема процесса менеджмента рисков. Установление контекста менеджмента риска.
28. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Критерии оценки, воздействия и принятия риска.
29. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Общее описание оценки рисков ИБ: идентификация активов, угроз, уязвимостей, средств защиты
30. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». методология измерения риска
31. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Обработка риска. Мониторинг и пересмотр, передача и принятие риска.
32. Методика Practical Threat Analysis.
33. Методика vsRisk.
34. Принятие решений по результатам оценки рисков. Политика обработки рисков

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-3. Способность выполнять работы по созданию (модификации) и сопровождению информационных систем и обеспечению их информационной безопасности.				
1.	Задание закрытого типа	Связь между достигнутым результатом и тем, насколько целесообразно использованы ресурсы 1) Эффективность 2) Цена 3) Стоимость 4) Актив	1	2
2.		Риск, возникающий вследствие политических, экономических факторов, связанный с резким изменением курса валюты 1. валютный 2. инфляционный 3. системный 4. общий	1	3
3.		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
4.		Экономическая модель позволяет оценить: 1. стоимость ущерба от реализации некоторой атаки 2. вероятность успешной атаки 3. эшелонирование средств защиты 4. информационный актив	1	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
5.		Вероятностная модель позволяет оценить: 1. стоимость ущерба от реализации некоторой атаки 2. вероятность успешной атаки 3. эшелонирование средств защиты 4. информационный актив	2	3
6.	Задание открытого типа	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.	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: $$П_В = П_{ВИ} + П_{ПВ} + П_{ЗЧ} = 1000 + 208{,}33 + 0 = 1208{,}33(ден.ед.)$$ Выгода: $$V = \frac{О_{ПР}}{52 \cdot 5 \cdot 8} \cdot (t_П + t_В + t_{ВИ}) = \frac{1000000 \cdot (2+8+8)}{2080} = 8653{,}85(ден.$$ 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.	5
7.		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 защит-	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

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		ная мера преодолевается с вероятностью 0,01. Защитные меры 7, 8, 9 не используются.		
8.		Какие отчеты формируются в PTA, позволяющие получить более подробную информацию о проведенном анализе рисков, кроме обобщенного отчета (пункт меню Reports → All Reports)	Кроме обобщенного отчета в PTA 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; Детализированный перечень контрмер; Наиболее опасные угрозы. Отчет самодиагностики: Полнота модели.	8
9.		Неценовые факторы, определяющие цену информации по степени важности	Неценовые факторы, определяющие цену информации по степени важности: первая группа факторов - риск, новизна, достоверность и полнота; вторая группа факторов - своевременность, конфиденциальность (наличие или отсутствие копий), приемлемая форма подачи.	8
10.		Спрос на информацию	Спрос на информацию порождается желанием субъекта снять или уменьшить риск или неопределенность той или иной ситуации. Спрос на информацию растет с возрастанием степени риска.	8

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.

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*	6/10	60	В соответствии с таблицей 2
2.	*Выполнение контрольной работы*	2/5	10	
3.	*Тест*	1/5	5	
4.	*Задача*	2/5	10	
5.	*Обзор методик*	1/5	5	
Всего			**90**	-
Блок бонусов				
6.	*Посещение занятий без пропусков*		3	
7.	*Своевременное выполнение всех заданий*		3	
8.	*Активность студента на занятии*		4	
Всего			**10**	-
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
60–100	зачтено
Ниже 60	незачтено

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

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).