**Федеральное государственное бюджетное**

**образовательное учреждение высшего образования**

**«Астраханский государственный университет имени В.Н. Татищева»**

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНО  Руководитель программы аспирантуры  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.М. Ажмухамедов  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2023 г. |  | УТВЕРЖДАЮ  Заведующий кафедрой ИТиК  *(наименование)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Марьенков  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**АНАЛИЗ РИСКОВ**

|  |  |
| --- | --- |
|  |  |
| Составитель(-и) | **Выборнова О.Н., к.т.н., доцент кафедры ИТиК; Ажмухамедов И.М., профессор, д.т.н., профессор кафедры ИТиК** |
| Группа научных специальностей | **2. 3. 6 Информационные технологии и телекоммуникации** |
| Научная специальность | **Методы и системы защиты информации, информационная безопасность** |
| Форма обучения | **очная** |
| Год приема  Срок освоения | **2023**  **3 года** |

Астрахань – 2023

**1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

**1.1. Целями освоения дисциплины** **(модуля)** «Анализ рисков» являются: освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности.

**1.2. Задачи освоения дисциплины (модуля):** «Анализ рисков»

- изучение современных методов и моделей анализа и оценки информационной безопасности объектов;

- умение анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия и проводить экспериментальные исследования защищенности объектов.

- изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности;

- изучение основных требований по управлению рисками информационной безопасности;

- формирование умений оценки и обработки рисков информационной безопасности;

- формирование навыков по оценке угроз безопасности информации в технологии оценки рисков;

- формирование навыков подбора инструментальных средств для управления рисками информационной безопасности.

**2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Освоение дисциплины (модуля) «Анализ рисков» направлено на достижение следующих результатов, определенных программой подготовки научных и научно-педагогическим кадров в аспирантуре:

- уметь анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им;

- уметь проводить экспериментальные исследования защищённости объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента;

- моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты;

-самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты.

**3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Общая трудоемкость дисциплины составляет – 4 зачетные единицы, 144 академических часов. На контактную работу обучающихся с преподавателем (по видам учебных занятий) – 28 часов и на самостоятельную работу обучающихся – 116 часов.

**Таблица 1.**

**Структура и содержание дисциплины (модуля)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование радела (темы) | Семестр | Неделя семестра | Контактная работа  (в часах) | | | Самостоят. работа | Формы текущего контроля успеваемости *(по неделям семестра)*  Форма промежуточной аттестации *(по семестрам)* |
| Л | ПЗ | ЛР |
|  | Цели и стандарты защиты информации. Расчет области оценки рисков. | 3 | 1-2 | 4 | 4 |  | 26 | Устный опрос  Практическое задание 1 |
|  | Разработка отчетных документов технологии анализа и управления рисками. | 3 | 3 | 2 | 2 |  | 18 | Устный опрос  Практическое задание 2 |
|  | Современные информационные риски и их особенности. | 3 | 4 | 2 | 2 |  | 18 | Устный опрос. |
|  | Система управления информационными рисками. | 3 | 5 | 2 | 2 |  | 18 |  |
|  | Обзор методов и инструментальных средств управления рисками: | 3 | 6 | 2 | 2 |  | 18 | Практическое задание 3 |
|  | Внедрение системы прогнозирования и управления рисками информационной безопасности. | 3 | 7 | 2 | 2 |  | 18 | Итоговое тестирование |
| **ИТОГО** | |  |  | **14** | **14** |  | **116** | **ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ** |

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы;

СР – самостоятельная работа по отдельным темам

**Содержание дисциплины**

**Цели и стандарты защиты информации.** **Расчет области оценки рисков.**

Принципы построения, модель и уровни зрелости процессов менеджмента информационной безопасности. Методы оценки ценности информационных ресурсов и идентификация перечня угроз, оценка их уровней и идентификации списка потенциальных уязвимостей. Расчет области оценки рисков.

**Разработка отчетных документов технологии анализа и управления рисками.** Основные сценарии, приводящие к различным негативным последствиям. Предпосылки для управления информационными рисками

**Современные информационные риски и их особенности.**

Кибертерроризм. Риски промышленных систем. Стандарты управления рисками. Государственное регулирование. Основные требования по управлению рисками информационной безопасности.

**Система управления информационными рисками.**

Оценка рисков информационной безопасности. Оценка угроз безопасности информации в технологии оценки рисков. Обработка рисков информационной безопасности. Инструментальные средства для управления рисками.

**Обзор методов и инструментальных средств управления рисками**:

Методики и программные продукты по управлению рисками OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.

**Внедрение системы прогнозирования и управления рисками информационной безопасности.**

Особенности внедрения системы управления информационными рисками (СУИР). Документация. Обучение членов экспертной группы. Проведение полной оценки рисков по всем активам. Жизненный цикл управления рисками.

**4. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ   
ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**

**4.1. Указания по организации и проведению лекционных, практических (семинарских) и лабораторных занятий с перечнем учебно-методического обеспечения**

Обучающемся проводится лекция с коллективным исследованием. По ходу излагаемого материала обучающимся предлагается совместно вывести то или иное правило, комплекс требований, определить закономерность на основе имеющихся знаний. Подводя итог рассуждениям, предложениям аспирантов, преподаватель дает правильное решение путем постановки необходимого вопроса.

Цель семинарских и практических занятий углубить и закрепить соответствующие знания аспирантов по предмету, но и развить инициативу, творческую активность, вооружить будущего специалиста методами и средствами научного познания. С точки зрения методики проведения семинар представляет собой комбинированную, интегративную форму учебного занятия. Он предполагает возможность использования рефератов.

**4.2. Указания для обучающихся по освоению дисциплины (модулю)**

**Таблица 2.**

**Содержание самостоятельной работы обучающихся**

|  |  |  |  |
| --- | --- | --- | --- |
| Номер радела (темы) | Темы/вопросы, выносимые на самостоятельное изучение | Кол-во  часов | Формы работы |
| Цели и стандарты защиты информации. Расчет области оценки рисков. | Нормативно-правовые документы в области управления рисками. ISO-15408:2002 «Общие критерии». | 26 | Внеаудиторная,  изучение учебных пособий |
| Разработка отчетных документов технологии анализа и управления рисками. | Методы управления рисками ИБ – ISO/IEC 27005:2011. | 18 | Внеаудиторная,  изучение учебных пособий |
| Современные информационные риски и их особенности. | Существующие подходы по анализу и управлению ИБ | 18 | Внеаудиторная,  изучение учебных пособий |
| Система управления информационными рисками. | Управление рисками в системе информационных технологий - NIST SP800-30. Оценка рисков ИБ – ENISA. | 18 | Внеаудиторная,  изучение учебных пособий |
| Обзор методов и инструментальных средств управления рисками: | Методика компании Microsoft. | 18 | Внеаудиторная,  изучение учебных пособий |
| Внедрение системы прогнозирования и управления рисками информационной безопасности. | Принятие решений по результатам оценки рисков. Политика обработки рисков. | 18 | Внеаудиторная,  изучение учебных пособий |

**4.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно** – не предусмотрено .

**5. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

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

**5.1. Образовательные технологии**

В рамках изучения дисциплины «Анализ рисков» предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий:

| Название образовательной технологии | Темы, разделы дисциплины | Краткое описание применяемой технологии |
| --- | --- | --- |
| Анализ проблемных ситуаций | По всем темам | Анализ проблемных ситуаций, выбор наиболее рациональных математических методов и моделей для обеспечения информационно-аналитической поддержки соответствующих решений, запись математических моделей на бумаге или в электронной форме, определение целесообразных численных методов для реализации разработанных математических моделей |
| Проведение сеансов видеоконференцсвязи | По всем темам | Использования сеансов видеоконференцсвязи для оперативного обсуждения с аспирантами вопросов, относящихся к теме курса |
| Изучение «свежих» статей, публикуемых в научных журналах университета | По всем темам | Используются свежие статьи, опубликованные в журналах Астраханского государственного университета (с целью анализа содержащейся в них информации, изучения новых методов и подходов к анализу данных) |
| Подготовка научных публикаций | По всем темам | С помощью преподавателя подготавливаются тексты научных публикаций, связанные с темой кандидатской диссертации |
| Решение практических задач расчетного характера с использованием штатных средств электронных таблиц и разработки программ для ЭВМ | По всем темам | Используются индивидуализированные постановки задач для решения на аудиторных занятиях |

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

**5.2. Информационные технологии**

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка 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 интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в глобальной сети (веб-конференции, форумы, учебно-методические материалы и др.));

- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс)

- использование виртуальной обучающей среды (или системы управления обучением LМS Moodle) или иных информационных систем, сервисов и мессенджеров.

|  |  |  |
| --- | --- | --- |
| Название информационной технологии | Темы, разделы дисциплины | Краткое описание  применяемой технологии |
| Использование возможностей Интернета в учебном процессе | По всем темам | Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах электронного обучения) |
| Использование средств представления учебной информации | По всем темам | Использование мультимедийной презентации |

**5.3. Перечень программного обеспечения и информационных справочных систем**

***Лицензионное программное обеспечение***

|  |  |
| --- | --- |
| Наименование программного обеспечения | Назначение |
| Adobe Reader | Программа для просмотра электронных документов |
| Mozilla FireFox | Браузер |
| Microsoft Office 2013,  Microsoft Office Project 2013, Microsoft Office Visio 2013 | Пакет офисных программ |
| 7-zip | Архиватор |
| Microsoft Windows 7 Professional | Операционная система |
| Kaspersky Endpoint Security | Средство антивирусной защиты |
| Платформа дистанционного обучения LМS Moodle | Виртуальная обучающая среда |

***Современные профессиональные базы данных, информационные справочные системы***

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: [https://library.asu.edu.ru](https://library.asu.edu.ru/).
2. Электронный каталог «Научные журналы АГУ»: <http://journal.asu.edu.ru/>.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: <http://dlib.eastview.com/>
4. Электронно-библиотечная система elibrary. <http://elibrary.ru>
5. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) [http://mars.arbicon.ru](http://mars.arbicon.ru/)
6. Электронные версии периодических изданий, размещенные на сайте информационных ресурсов [www.polpred.com](http://www.polpred.com)
7. Справочная правовая система КонсультантПлюс: [http://www.consultant.ru](http://www.consultant.ru/)
8. Информационно-правовое обеспечение «Система ГАРАНТ»: [http://garant-astrakhan.ru](http://garant-astrakhan.ru/)

***Перечень международных реферативных баз данных научных изданий*** – не используются.

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

**6.1. Паспорт фонда оценочных средств**

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Анализ рисков» проверяется сформированность у обучающихся планируемых результатов обучения,указанных в разделе 2 настоящей программы*.*

**Таблица 3.**

**Соответствие разделов, тем дисциплины (модуля),**

**результатов обучения по дисциплине (модулю) и оценочных средств**

|  |  |  |
| --- | --- | --- |
| № п/п | Контролируемые разделы (этапы) | Наименование  оценочного средства |
| 1 | Цели и стандарты защиты информации. Расчет области оценки рисков. | Вопросы для обсуждения.  Практическое задание 1 |
| 2 | Разработка отчетных документов технологии анализа и управления рисками. | Вопросы для обсуждения  Практическое задание 2 |
| 3 | Современные информационные риски и их особенности. | Вопросы для обсуждения. |
| 4 | Система управления информационными рисками. | Вопросы для обсуждения |
| 5 | Обзор методов и инструментальных средств управления рисками: | Вопросы для обсуждения.  Практическое задание 3 |
| 6 | Внедрение системы прогнозирования и управления рисками информационной безопасности. | Вопросы для обсуждения. Итоговое тестирование. Вопросы к зачету |

**6.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

**Таблица 4**

**Показатели оценивания результатов обучения**

|  |  |
| --- | --- |
| Шкала оценивания | Критерии оценивания |
| 5  «отлично» | демонстрирует глубокое знание теоретического материала при выполнении заданий; последовательно и правильно выполняет задания;  обоснованно излагает свои мысли и делает необходимые выводы;  правильно и аргументированно отвечает на вопросы, приводит примеры. |
| 4  «хорошо» | демонстрирует знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания;  обоснованно излагает свои мысли и делает необходимые выводы;  допускает единичные ошибки, исправляемые после замечания преподавателя. |
| 3  «удовлетворительно» | демонстрирует отдельные, несистематизированные знания, 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» | демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры |

**6.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения**

**Цели и стандарты защиты информации.** **Расчет области оценки рисков.**

***1. Вопросы для обсуждения***

1. Цели и стандарты защиты информации
2. Принципы построения, модель и уровни зрелости процессов менеджмента информационной безопасности.
3. Методы оценки ценности информационных ресурсов и идентификация перечня угроз, оценка их уровней и идентификации списка потенциальных уязвимостей.
4. Расчет области оценки рисков.

***2. Практическое задание 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.

**Разработка отчетных документов технологии анализа и управления рисками.**

***1. Вопросы для обсуждения***

1. Разработка отчетных документов технологии анализа и управления рисками.
2. Основные сценарии, приводящие к различным негативным последствиям.
3. Предпосылки для управления информационными рисками.

***2. Практическое задание 2 (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.

**Современные информационные риски и их особенности.**

***1. Вопросы для обсуждения***

1. Современные информационные риски и их особенности.
2. Кибертерроризм.
3. Риски промышленных систем.
4. Стандарты управления рисками.
5. Государственное регулирование.
6. Основные требования по управлению рисками информационной безопасности.

**Система управления информационными рисками.**

***1. Вопросы для обсуждения***

1. Система управления информационными рисками.
2. Оценка рисков информационной безоасности.
3. Оценка угроз безопасности информации в технологии оценки рисков.
4. Обработка рисков информационной безопасности.
5. Инструментальные средства для управления рисками.

**Обзор методов и инструментальных средств управления рисками**:

***1. Вопросы для обсуждения***

1. Обзор методов и инструментальных средств управления рисками:
2. Методики и программные продукты по управлению рисками OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.

***2. Практическое задание 3. Обзор методик оценки рисков***

Оформить таблицу

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

**Внедрение системы прогнозирования и управления рисками информационной безопасности.**

***1. Вопросы для обсуждения***

1. Внедрение системы прогнозирования и управления рисками информационной безопасности.
2. Особенности внедрения системы управления информационными рисками (СУИР).
3. Документация.
4. Обучение членов экспертной группы.
5. Проведение полной оценки рисков по всем активам.
6. Жизненный цикл управления рисками.

***2. Итоговое тестирование*** (Примерные тестовые задания)

1. Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу и его несанкционированного использования
2. Атака
3. Актив
4. Угроза
5. Воздействие
6. Систематическое использование информации для выявления источников и оценки риска
7. Атака
8. Анализ риска
9. Угроза
10. Воздействие
11. Сочетание вероятности события и его последствий
12. Риск
13. Атака
14. Актив
15. Угроза
16. Возможная причина нежелательного инцидента, который может нанести ущерба системе или организации
17. Атака
18. Анализ
19. Угроза
20. Воздействие
21. Слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой
22. Уязвимость
23. Риск
24. Атака
25. Актив

**Вопросы для зачета:**

1. Цели и стандарты защиты информации.
2. Принципы построения, модель и уровни зрелости процессов менеджмента информационной безопасности.
3. Методы оценки ценности информационных ресурсов и идентификация перечня угроз, оценка их уровней и идентификации списка потенциальных уязвимостей.
4. Расчет области оценки рисков.
5. Разработка отчетных документов технологии анализа и управления рисками.
6. Основные сценарии, приводящие к различным негативным последствиям.
7. Предпосылки для управления информационными рисками
8. Современные информационные риски и их особенности.
9. Кибертерроризм. Риски промышленных систем.
10. Стандарты управления рисками.
11. Государственное регулирование. Основные требования по управлению рисками информационной безопасности.
12. Система управления информационными рисками.
13. Оценка рисков информационной безопасности.
14. Оценка угроз безопасности информации в технологии оценки рисков. Обработка рисков информационной безопасности.
15. Инструментальные средства для управления рисками. Обзор методов и инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.
16. Внедрение системы прогнозирования и управления рисками информационной безопасности.
17. Особенности внедрения системы управления информационными рисками (СУИР). Документация.
18. Обучение членов экспертной группы.
19. Проведение полной оценки рисков по всем активам.
20. Жизненный цикл управления рисками.

**6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Оценивание аспирантов осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Зачет основан на итоговой оценке, включающий в себя следующее: суммы баллов по результатам текущего контроля (устные опросы, контрольные задания, комплексное задание творческого (проблемного) характера; результаты работы на занятиях в процессе обучения (инициативность, качество выполнения текущих заданий и пр.); результаты итогового тестирования; количества пропусков занятий; публикационная активность по теме учебного курса.

Преподаватель, реализующий дисциплину, в зависимости от уровня подготовленности, обучающихся может использовать иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

**7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ   
ДИСЦИПЛИНЫ (МОДУЛЯ)**

**а) 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).

**б) 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»).

**в) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины (модуля)**

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" <http://www.studentlibrary.ru/>
2. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru

**8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Вуз располагает необходимыми материально-техническими условиями для качественного проведения учебного процесса по реализуемой ОПОП ВО. Материально-техническое обеспечение включает необходимые учебные и вспомогательные площади для учебного процесса, достаточную инфраструктуру, обеспечение учебного процесса вычислительной и оргтехникой, достаточным количеством учебных материалов. Все учебные помещения оборудованы соответствующей мебелью, досками, техническими средствами обучения, что позволяет качественно осуществлять учебный процесс.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление аспиранта (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).