

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан ФИТКБ

/Гусев П.Ю./

31.08.2021 г.

«Меры и методология оценки информационных рисков нарушения  
безопасности»

**Направление подготовки** 10.06.01 ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ

**Профиль** 05.13.19 Методы и системы защиты информации,  
информационная безопасность

**Квалификация выпускника** Исследователь. Преподаватель-исследователь

**Нормативный период обучения** 4 года

**Форма обучения** очная

**Год начала подготовки** 2021

Автор программы  В.И. Белоножкин

Заведующий кафедрой  
Систем информационной  
безопасности  А.Г. Остапенко

Руководитель ОПОП  А.Г. Остапенко

Воронеж 2021

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1. Цели дисциплины

теоретическая и практическая подготовка по вопросам оценки рисков нарушения безопасности систем и сетей.

### 1.2. Задачи освоения дисциплины

– изучение теоретических основ стохастичности защиты информации в средствах вычислительной техники и автоматизированными системами;

– изучение теоретических основ оценки ущербов и частоты нарушения защищенности информации;

– изучение теоретических основ методов и средств оценки и контроля рисков и эффективности защиты информации и обеспечения безопасности систем и сетей.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Меры и методология оценки информационных рисков нарушения безопасности» относится к дисциплинам вариативной части блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Меры и методология оценки информационных рисков нарушения безопасности» направлен на формирование следующих компетенций:

ОПК-1 - способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность

ПК-3 - способность пользоваться мерами риска и владение методами оценки информационных рисков

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	знать принципы построения защищенных распределенных компьютерных систем и сетей; теоретические основы недетерминированных процессов нарушения безопасности информации; возможности нечетких и случайных переменных информации
	уметь формализовать задачу управления безопасностью информационных систем
	владеть методами контроля и эффективности защиты информации
ПК-3	знать рискованные основы способов и средств защиты информации и минимизации информационных рисков, контроля эффективности защиты информации
	уметь оценивать защищенность систем
	владеть навыками проведения измерения и анализа рисков и администрирования безопасности распределенных компьютерных систем

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Меры и методология оценки информационных рисков нарушения безопасности» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий  
**очная форма обучения**

Виды учебной работы	Всего часов	Семестры
		4
<b>Аудиторные занятия (всего)</b>	18	18
В том числе:		
Лекции	18	18
<b>Самостоятельная работа</b>	90	90
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	108 3	108 3

#### 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий  
**очная форма обучения**

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	<i>Оценка риска информационной безопасности</i>	Анализ риска. Оценивание рисков. Измерение рисков.	4	4	6	14
2	<i>Риски информационных систем: обзор современных стандартов и методов оценки и управления</i>	Анализ современных стандартов в области управления рисками информационных систем. Анализ международного стандарта ISO IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005) в области управления рисками информационной безопасности. Анализ международного стандарта ISO IEC 27001 (ГОСТ Р ИСО/МЭК 27001-2005) в области мониторинга и управления рисками информационной безопасности. Анализ британского стандарта BS 7799-3 «Руководство по управлению информационными рисками». Анализ стандарта США NIST 800-30 «Руководство по управлению информационными рисками IT-систем».	6	6	8	20
3	<i>Аналитический подход в методологии оценки и управления рисками: обобщение и пути развития</i>	Понятие риска системы. Концепции оценки рисков. Обобщенная модель оценки риска. Вероятностная природа риска. Методы оценки	4	4	6	14

		риска. Формальное определение меры риска. Основные меры риска, используемые в анализе информационных систем. Методы оптимизации вычислений при расчете риска систем. Объективные и субъективные составляющие риска систем. Аналитические методы управления рисками. Понятие и обобщенная схема управления рисками. Принципы принятия решений по управлению рисками. Основные критерии выбора оптимальных решений по управлению рисками.				
4	<i>Развитие методического обеспечения оценки риска информационных систем</i>	Постановка задачи оценки риска информационной системы. Общий вид модели оценки риска информационных систем. Применение кластерного анализа при оценке рисков информационной системы. Формализация оценки риска информационной системы. Критерий принятия решений по управлению рисками на основе функции полезности.	2	2	4	8
5	<i>Алгоритмизация и практическое применение методики управления рисками информационных систем на базе интересо-ориентированного подхода</i>	Алгоритмы управления рисками информационных систем.	2	2	4	8
6	<i>Коммуникации риска информационной безопасности</i>	Коммуникации риска информационной безопасности.	2	2	4	8
7	<i>Мониторинг и переоценка риска информационной безопасности</i>	Мониторинг и переоценка факторов риска.	2	2	4	8
8	<i>Аналитическая формализация ущерба и риска превышения пороговых значений критических переменных состояния</i>	Пути аналитического развития инструментария оценки рисков. Параметры и характеристика риска для одной переменной состояния.	4	4	6	14
9	<i>Риски и защищенность систем для непрерывных распределений вероятности ущерба</i>	Оценка рисков и защищенности систем для нормального непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для равномерного непрерывного распределения вероятностей ущерба.	4	4	6	14
<b>Итого</b>			<b>30</b>	<b>30</b>	<b>48</b>	<b>108</b>

## 5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

## 6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

**7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

### 7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-1	знать принципы построения защищенных распределенных компьютерных систем и сетей; теоретические основы недетерминированных процессов нарушения безопасности информации; возможности нечетких и случайных переменных информации	знание принципов построения защищенных распределенных компьютерных систем и сетей; теоретические основы недетерминированных процессов нарушения безопасности информации; возможности нечетких и случайных переменных информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь formalизовать задачу управления безопасностью информационных систем	умение formalизовать задачу управления безопасностью информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами контроля и эффективности защиты информации	владение методами контроля и эффективности защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-3	знать рискованные основы способов и средств защиты информации и минимизации информационных рисков, контроля эффективности защиты информации	знание рискованных основ способов и средств защиты информации и минимизации информационных рисков, контроля эффективности защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать защищенность систем	умение оценивать защищенные системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

			рабочих программах	в рабочих программах
	владеть навыками проведения измерения и анализа рисков и администрирования безопасности распределенных компьютерных систем	владение навыками проведения измерения и анализа рисков и администрирования безопасности распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	знать принципы построения защищенных распределенных компьютерных систем и сетей; теоретические основы недетерминированных процессов нарушения безопасности информации; возможности нечетких и случайных переменных информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь формализовать задачу управления безопасностью информационных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть методами контроля и эффективности защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-3	знать рискованные основы способов и средств защиты информации и минимизации информационных рисков, контроля эффективности защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь оценивать защищенность систем	Решение стандартных практических	Задачи решены в полном	Продемонстрирован верный ход	Продемонстрирован верный ход	Задачи не решены

		задач	объеме и получены верные ответы	решения всех, но не получен верный ответ во всех задачах	решения в большинстве задач	
владеть навыками проведения измерения и анализа рисков и администрирования безопасности распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены	

## 7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

### 7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Что в сфере информационной безопасности принято считать риском?
  - (1) потенциальную возможность понести убытки из-за нарушения безопасности информационной системы
  - (2) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней
  - (3) характеристику, которая делает возможным возникновение угрозы
2. Что отличает риск от угрозы?
  - (1) объем вероятных потерь
  - (2) наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы
  - (3) угроза и риск - понятия идентичные
3. Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?
  - (1) да
  - (2) нет
  - (3) да, но только в случае отсутствия угрозы
4. Какие из перечисленных вариантов решений в отношении рисков являются неуместными:
  - (1) принят, устранен
  - (2) принят, дезавуирован
  - (3) дезавуирован, отклонен
5. В каком отечественном документе впервые в России выделено понятие риска в отношении ИБ?
  - (1) ГОСТ Р ИСО/МЭК 15408-2002
  - (2) КЗОТ
  - (3) УК РФ
6. Какое из перечисленных требований доверия к безопасности не является справедливым?
  - (1) к технологии разработки и тестированию

(2) к анализу уязвимостей

**(3) верификации контента**

7. На основании каких из перечисленных документов разрабатываются задания по безопасности?

(1) каталог сертифицированных профилей защиты и продуктов

(2) технический регламент

**(3) профиль защиты**

8. Какая модель используется для количественных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер?

(1) функциональная модель

**(2) математическая модель**

(3) концептуальная модель

(4) теоретическая модель

9. К какому аспекту мероприятий по защите информации относится определение на основе нормативных документов требований по категорированию информации?

**(1) законодательный**

(2) организационный

(3) программно-технический

10. К какому аспекту мероприятий по защите информации относится формирование политики информационной безопасности?

(1) законодательный

**(2) организационный**

(3) программно-технический

### **7.2.2 Примерный перечень заданий для решения стандартных задач**

1. Какие из перечисленных факторов, предписано учитывать в ГОСТ Р ИСО/МЭК 17799:2005 при формировании требований безопасности?

**(1) оценку рисков организации**

**(2) юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг**

**(3) специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации**

2. Может организация в целях обеспечения безопасности разрабатывать свой специфический набор принципов, целей и требований, в отношении обработки информации?

**(1) да, безусловно**

(2) нет

(3) да, но только по согласованию с местными органами власти

3. Что достигается посредством оценки рисков организации?

**(1) анализируется вероятность возникновения угроз, а также оценка возможных последствий**

**(2) происходит выявление угроз активам организации**

**(3) осуществляется изучение уязвимости соответствующих**

## **активов**

4. Каковы рекомендации стандарта по обучению пользователей процедурам безопасности?

**(1) всех пользователей необходимо обучать процедурам безопасности и правильному использованию средств обработки информации**

(2) всех пользователей не реже одного раза в год предписано обучать и экзаменовывать на предмет знаний процедур безопасности

(3) требования по процедурам безопасности доводятся единожды при приеме на работу под роспись, в дальнейшем контроля за знанием работником процедур безопасности не требуется

5. Входит в перечень рекомендаций по обеспечению физической защиты и защиты от воздействия окружающей среды организация зон безопасности?

**(1) да**

(2) нет

(3) нет, но имеется ссылка на требования законодательства

6. Для чего необходимо проводить мониторинг системы безопасности?

(1) в целях формирования требований политики контроля доступа

(2) в целях обеспечения релевантности действий сотрудников учреждения

**(3) в целях обеспечения доказательства на случай выявления инцидентов нарушения информационной безопасности**

7. В каких целях осуществляется анализ рисков?

(1) в целях соблюдения требований об обязательной отчетности учреждения, его проведение формально необходимо

**(2) в целях установления и поддержания эффективного управления системой защиты**

(3) в целях укрепления имиджевой политики учреждения

8. Какова связь анализа рисков с другими компонентами модели информационной безопасности?

**(1) на базе полученных результатов по оценке рисков осуществляется анализ состояния системы и разрабатывается план построения системы защиты сети**

(2) анализ рисков увязан с процедурами анализа рисков

(3) анализ не увязывается с другими компонентами системы

9. Сколько классов защищенности от НСД существует для АС?

(1) 3

(2) 5

**(3) 9**

(4) 15

10. На сколько групп подразделяются классы защищенности АС?

(1) 2

**(2) 3**

(3) 5

(4) 9

### **7.2.3 Примерный перечень заданий для решения прикладных задач**

1. Какая из перечисленных распространенных методик анализа рисков

использует метод оценки риска на качественном уровне (например, по шкале "высокий", "средний", "низкий")?

FRAP

RiskWatch

**CRAMM**

2. Какая из перечисленных распространенных методик анализа рисков использует количественные методики оценки рисков?

FRAP

**RiskWatch**

CRAMM

Microsoft

3. Какие из перечисленных распространенных методик анализа рисков используют смешанный метод оценки риска?

**CRAMM**

**Microsoft**

RiskWatch

FRAP

4. Сколько стадий исследование информационной безопасности системы имеется в методике CRAMM?

одна

две

**три**

четыре

5. Какому из перечисленных значений по шкале оценки уязвимости CRAMM соответствует инцидент, если вероятность развития событий по наихудшему сценарию составляет от 0,33 до 0,66?

высокий

низкий

**средний**

6. Как в методике FRAP осуществляется определение защищаемых активов?

по результатам заполнения опросных листов и автоматизированного анализа (сканирования) сетей

по результатам изучения документации на систему

**по результатам заполнения опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей**

7. Что из перечисленного характерно для методики OCTAVE?

весь процесс анализа автоматизирован, производится на основании параметрических функций

**весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов**

весь процесс анализа производится силами внешних консультантов, без привлечения сотрудников организации

8. Перечислите классы по которым принято производить классификацию

межсетевого экрана по принципу уровней фильтрации.

**экранирующий маршрутизатор**

**экранирующий транспорт (шлюз сеансового уровня)**

**экранирующий шлюз (шлюз прикладного уровня)**

экранирующий шлюз (шлюз внутреннего уровня)

9. Какую схему установки межсетевого экрана логично применить если требования в области защиты от несанкционированного межсетевого доступа примерно одинаковы для всех узлов внутренней сети?

схема, в которой для защиты сети с DMZ задействуются два независимо конфигурируемых межсетевых экрана

**схема установки в которой межсетевой экран устанавливается после маршрутизатора**

схема использования межсетевого экрана с тремя сетевыми интерфейсами

10. К чему приводит установка флажка "Notify me when Windows Firewall blocks a new program" в панели управления?

отключается возможность полностью контролировать подключения в пределах внутреннего сегмента межсетевого экрана

**при наличии проблем в ходе установки нового приложения, пользователь информируется о том, что брандмауэр не позволяет его устанавливать**

подключения к узлам открытого сегмента межсетевого экрана контролируются лишь избирательно

### **7.2.5 Примерный перечень заданий для подготовки к экзамену**

1. Применение кластерного анализа при оценке рисков информационной системы.
2. Формализация оценки риска информационной системы.
3. Критерий принятия решений по управлению рисками на основе функции полезности.
4. Развитие интересо-ориентированного подхода к оценке и управлению рисками информационных систем.
5. Учет динамики развития информационных систем в управлении рисками.
6. Оценка рисков и защищенности систем для нормального непрерывного распределения вероятностей ущерба.
7. Оценка рисков и защищенности систем для непрерывного нормального выборочного U-распределения вероятностей ущерба.
8. Оценка рисков и защищенности систем для непрерывного нормального выборочного t-распределения вероятностей ущерба.
9. Оценка рисков и защищенности систем для  $\chi^2$  непрерывного распределения вероятностей ущерба.
10. Оценка рисков и защищенности систем для логарифмически нормального непрерывного распределения вероятностей ущерба.
11. Оценка рисков и защищенности систем для непрерывного Лапласа распределения вероятностей ущерба.

12. Оценка рисков и защищенности систем для непрерывного  $\beta$ -распределения вероятностей ущерба.

13. Оценка рисков и защищенности систем для непрерывного гамма-распределения вероятностей ущерба.

14. Оценка рисков и защищенности систем для непрерывного экспоненциального распределения вероятностей ущерба.

15. Оценка рисков и защищенности систем для равномерного непрерывного распределения вероятностей ущерба.

#### **7.2.6. Методика выставления оценки при проведении промежуточной аттестации**

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

#### **7.2.7 Паспорт оценочных материалов**

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	<i>Оценка риска информационной безопасности</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	<i>Риски информационных систем: обзор современных стандартов и методов оценки и управления</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	<i>Аналитический подход в методологии оценки и управления рисками: обобщение и пути развития</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	<i>Развитие методического обеспечения оценки риска информационных систем</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	<i>Алгоритмизация и практическое применение методики управления рисками информационных систем на базе</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата,

	<i>интересо-ориентированного подхода</i>		требования к курсовому проекту....
6	<i>Коммуникации риска информационной безопасности</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
7	<i>Мониторинг и переоценка риска информационной безопасности</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
8	<i>Аналитическая формализация ущерба и риска превышения пороговых значений критических переменных состояния</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
9	<i>Риски и защищенность систем для непрерывных распределений вероятности ущерба</i>	ОПК-1, ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....

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

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методике выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

## **8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)**

### **8.1 Перечень учебной литературы, необходимой для освоения дисциплины**

#### *Основная литература*

Остапенко А.Г. Теория сетевых войн: живучесть атакуемых сетей: учебное пособие, 2015.

Остапенко Г.А. Методическое обеспечение оценки и регулирования

рисков распределенных информационных систем: учеб. пособие, 2011.

Остапенко А.Г., Плотников Д.Г., Машин С.В. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением: учеб. пособие 2012.

*Дополнительная литература*

Милославская Н.Г. Управление рисками информационной безопасности: учебное пособие 2014.

Милославская Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие 2014.

*Методические разработки*

Дешина А.Е. Методические указания к практическим занятиям по дисциплине «Меры и методология оценки информационных рисков нарушения безопасности» для аспирантов направления подготовки 10.06.01 «Информационная безопасность» очной формы обучения.

Соколова Е.С., Остапенко О.А. Методические указания к самостоятельным занятиям по дисциплине «Меры и методология оценки информационных рисков нарушения безопасности» для аспирантов направления подготовки 10.06.01 «Информационная безопасность» очной формы обучения.

**8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:**

Программа CVE ®. Выявление, определение и каталогизация публично раскрытых уязвимостей в области кибербезопасности

<https://cve.mitre.org/>

База знаний о тактике и методах противника, основанная на наблюдениях в реальном мире, которая используется в качестве основы для разработки конкретных моделей угроз и методологий в частном секторе, в правительстве и в сообществе продуктов и услуг кибербезопасности.

<https://attack.mitre.org/>

Сайт ФСТЭК России

<https://fstec.ru/>

Банк данных угроз безопасности информации

<https://bdu.fstec.ru/vul>

Информационный портал компании Positive Technologies

<https://www.securitylab.ru/>

Средство оценки рисков, предоставляющее информацию о системе безопасности ИТ-инфраструктуры и рекомендации по ее улучшению Microsoft Security Assessment Tool

<https://www.microsoft.com/ru-RU/download/details.aspx?id=12273>

CORAS Tool программная реализация методологии Coras, предназначенная для анализа рисков безопасности, представляет собой инструмент для моделирования рисков и угроз

[https://coras.sourceforge.net/coras\\_tool.html](https://coras.sourceforge.net/coras_tool.html)

Сборник программ по риск-менеджменту

<https://www.softwareadvice.co.uk/directory/m218/risk-management/software>

Руководство по методология управления, контроля и аудита информационных систем (СОБИТ) разработана Международной ассоциацией аудита и контроля за информационными системами (ISACA)

<https://ea-banks.ucoz.ru/load/3-1-0-3>

Список экстремистских материалов

<https://minjust.gov.ru/ru/extremist-materials/>

Управление рисками информационной безопасности. Электронный ресурс

<http://mephi.edu/dist/magistracy/urib/ISRisks/Page44.htm>

Искусство управления информационными рисками. А. Астахов

<http://xn----7sbab7afcques2bn.xn--plai/>

vsRisk Программное обеспечение для оценки рисков информационной безопасности в соответствии с требованиями стандартов ISO 27001 и BS 7799-3

<https://www.itgovernance.co.uk/>

Интернет портал ISO27000.RU для общения менеджеров и экспертов по информационной безопасности, а также всех, кто интересуется вопросами защиты информации, компьютерной и сетевой безопасности, современным информационным законодательством и стандартами, риск-менеджментом, аудитом безопасности и смежными технологиями

<http://www.iso27000.ru/o-proekte>

Управление рисками информационной безопасности (конспект лекции)

<https://www.securityvision.ru/>

## **9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

Помещение для занятий лекционного типа. Лаборатория информационно-коммуникационных систем. Персональные компьютеры, подключенных к сети интернет, ученические столы, стулья.

## **10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

По дисциплине «Меры и методология оценки информационных рисков нарушения безопасности» читаются лекции.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов,

	<p>терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.</p>
<p>Самостоятельная работа</p>	<p>Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:</p> <ul style="list-style-type: none"> <li>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;</li> <li>- выполнение домашних заданий и расчетов;</li> <li>- работа над темами для самостоятельного изучения;</li> <li>- участие в работе студенческих научных конференций, олимпиад;</li> <li>- подготовка к промежуточной аттестации.</li> </ul>
<p>Подготовка к промежуточной аттестации</p>	<p>Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.</p>

