

**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



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**«Риск-анализ вирусных атак на информационно-  
телекоммуникационные системы и сети»**

**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		А.Г. Остапенко
Заведующий кафедрой Систем информационной безопасности		А.Г. Остапенко
Руководитель ОПОП		А.Г. Остапенко

Воронеж 2022

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1. Цели дисциплины

формирование сведений и представлений о методах и средствах риск-анализа вирусных атак на информационно-телекоммуникационные системы и сети управление их защищенностью.

### 1.2. Задачи освоения дисциплины

- знакомство с основными типами вирусных атак, особенностями их реализации и методах защиты от них;
- знакомство с методами риск-анализа информационно-телекоммуникационных систем и сетей при реализации в их отношении вирусных атак;
- изучение методологической базы в области управления рисками успешных реализаций вирусных атак на информационно-телекоммуникационные системы и сети.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Риск-анализ вирусных атак на информационно-телекоммуникационные системы и сети» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Риск-анализ вирусных атак на информационно-телекоммуникационные системы и сети» направлен на формирование следующих компетенций:

ОПК-2 - способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности

ПК-5 - способность проводить риск-анализ различных атак на информационно-телекоммуникационные системы и сети

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-2	знать особенности информационно-телекоммуникационных систем и сетей; способы и методы вирусного заражения элементов информационно-телекоммуникационных систем; способы и методы противодействия вирусному заражению элементов информационно-телекоммуникационных систем и сетей
	уметь осуществлять анализ и систематизацию полученных при моделировании результатов; регулировать показатели эффективности защиты информационно-телекоммуникационных систем и сетей
	владеть навыками моделирования вирусных атак на информационно-телекоммуникационных системы и сети
ПК-5	знать методы оценки и способы регулирования риска

	информационно-телекоммуникационных систем и сетей
	уметь подбирать математический аппарат и проводить моделирование вирусных атак на информационно-телекоммуникационные системы и сети
	владеть методологией оценки и регулирования риска вирусно-атакуемых информационно-телекоммуникационных систем и сетей

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Риск-анализ вирусных атак на информационно-телекоммуникационные системы и сети» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

##### очная форма обучения

Виды учебной работы	Всего часов	Семестры
		5
<b>Аудиторные занятия (всего)</b>	10	10
В том числе:		
Лекции	10	10
в том числе в форме практической подготовки	4	4
<b>Самостоятельная работа</b>	98	98
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость:		
академические часы	108	108
зач.ед.	3	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>Анализ разновидностей вирусных атак и исследование особенностей распространения вирусных эпидемий.</i>	Многообразие вредоносного программного обеспечения вирусного характера. Особенности реализации вирусных атак на разнообразные информационно-телекоммуникационные системы.	2	2	6	10
2	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение файловым вирусом, заражение сетевым вирусом.</i>	Заражение файловым вирусом. Заражение сетевым вирусом. Оценка вероятности заражения элемента конкретно взятой информационно-телекоммуникационной системы с использованием полученных моделей с использованием сетей Петри-Маркова.	2	2	8	12

3	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение загрузочным вирусом, макровирусом, скрипт-вирусом.</i>	Оценка вероятности заражения элементов информационно-телекоммуникационной системы загрузочным вирусом, макровирусом, скрипт-вирусом. Используемые протоколы передачи информации, реализовываемые рассматриваемые типы деструктивных информационных воздействий. Обоснование использования сети Петри-Маркова.	2	2	4	8
4	<i>Оценка вероятностей реализации различных этапов вирусной атаки.</i>	Вероятностная модель процесса инфекционного заражения элемента атакуемой информационно-телекоммуникационной системы. Вероятностная модель процесса излечения зараженного элемента атакуемой информационно-телекоммуникационной системы.	4	2	6	12
5	<i>Риск-анализ и оценка эпистойкости информационных систем в условиях распространения эпидемии по модели SI.</i>	Аналитические выражения для расчета количества зараженных и восприимчивых элементов атакуемой системы на различных этапах ее функционирования в условиях распространения эпидемии по модели SI.	4		8	12
6	<i>Риск-анализ и оценка эпистойкости информационных сетей в условиях распространения вирусной эпидемии по модели SIS.</i>	Аналитические выражения для расчета количества зараженных и восприимчивых элементов атакуемой системы на различных этапах ее функционирования в условиях распространения вирусной эпидемии по модели SIS. Аналитические выражения риска и эпистойкости атакуемой системы; Расчет риска и эпистойкость атакуемой системы с использованием пиковых и усредненных оценок в условиях распространения вирусной эпидемии по модели SIS.	4	2	2	8
7	<i>Риск-анализ и оценка эпистойкости информационных сетей в условиях распространения вирусной эпидемии по модели SEIS.</i>	Аналитические выражения для расчета количества зараженных и восприимчивых элементов атакуемой системы на различных этапах ее функционирования в условиях распространения вирусной эпидемии по модели SEIS. Аналитические выражения риска и эпистойкости атакуемой системы. Расчет риска и эпистойкость атакуемой системы с использованием пиковых и	4		6	10

		усредненных оценок в условиях распространения вирусной эпидемии по модели SEIS.				
8	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SIR.</i>	Аналитические выражения для расчета количества зараженных и восприимчивых элементов атакуемой системы на различных этапах ее функционирования в условиях распространения вирусной эпидемии по модели SIR. Аналитические выражения риска и эпистойкости атакуемой системы; Расчет риска и эпистойкость атакуемой системы с использованием пиковых и усредненных оценок в условиях распространения вирусной эпидемии по модели SIR.	4	2	8	14
9	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SEIR.</i>	Аналитические выражения для расчета количества зараженных и восприимчивых элементов атакуемой системы на различных этапах ее функционирования в условиях распространения вирусной эпидемии по модели SEIR. Аналитические выражения риска и эпистойкости атакуемой системы. Расчет риска и эпистойкость атакуемой системы с использованием пиковых и усредненных оценок в условиях распространения вирусной эпидемии по модели SEIR.	4	3	15	22
<b>Итого</b>			<b>30</b>	<b>15</b>	<b>63</b>	<b>108</b>

Практическая подготовка при освоении дисциплины (модуля) проводится путем непосредственного выполнения обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы на практических занятиях и (или) лабораторных работах:

№ п/п	Перечень выполняемых обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью	Формируемые профессиональные компетенции
1	<i>Анализ разновидностей вирусных атак и исследование особенностей распространения вирусных эпидемий</i>	ПК-5
2	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение файловым вирусом, заражение сетевым вирусом</i>	ПК-5

3	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение загрузочным вирусом, макровирусом, скрипт-вирусом</i>	ПК-5
4	<i>Оценка вероятностей реализации различных этапов вирусной атаки</i>	ПК-5
5	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SIS</i>	ПК-5
6	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SIR</i>	ПК-5
7	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SEIR</i>	ПК-5

## 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-2	знать особенности информационно-телекоммуникационных систем и сетей; способы и методы вирусного заражения элементов информационно-телекоммуникационных систем; способы и методы противодействия вирусному	знание особенностей информационно-телекоммуникационных систем и сетей; способы и методы вирусного заражения элементов информационно-телекоммуникационных систем; способы и методы противодействия вирусному заражению элементов	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	заражению элементов информационно-телекоммуникационных систем и сетей	информационно-телекоммуникационных систем и сетей		
	уметь осуществлять анализ и систематизацию полученных при моделировании результатов; регулировать показатели эффективности защиты информационно-телекоммуникационных систем и сетей	умение осуществлять анализ и систематизацию полученных при моделировании результатов; регулировать показатели эффективности защиты информационно-телекоммуникационных систем и сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками моделирования вирусных атак на информационно-телекоммуникационные системы и сети	владение навыками моделирования вирусных атак на информационно-телекоммуникационные системы и сети	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать методы оценки и способы регулирования риска информационно-телекоммуникационных систем и сетей	знание методов оценки и способов регулирования риска информационно-телекоммуникационных систем и сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь подбирать математический аппарат и проводить моделирование вирусных атак на информационно-телекоммуникационные системы и сети	умение подбирать математический аппарат и проводить моделирование вирусных атак на информационно-телекоммуникационные системы и сети	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методологией оценки и регулирования риска вирусно-атакуемых информационно-телекоммуникационных систем и сетей	владение методологией оценки и регулирования риска вирусно-атакуемых информационно-телекоммуникационных систем и сетей	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 5 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-2	знать особенности информационно-телекоммуникационных систем и сетей; способы и методы вирусного заражения элементов информационно-телекоммуникационных систем; способы и методы противодействия вирусному заражению элементов информационно-телекоммуникационных систем и сетей	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь осуществлять анализ и систематизацию полученных при моделировании результатов; регулировать показатели эффективности защиты информационно-телекоммуникационных систем и сетей	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками моделирования вирусных атак на	Решение прикладных задач в конкретной	Продемонстрирован верный ход	Задачи не решены

	информационно-телекоммуникационных системы и сети	предметной области	решения в большинстве задач	
ПК-5	знать методы оценки и способы регулирования риска информационно-телекоммуникационных систем и сетей	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь подбирать математический аппарат и проводить моделирование вирусных атак на информационно-телекоммуникационные системы и сети	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть методологией оценки и регулирования риска вирусно-атакуемых информационно-телекоммуникационных систем и сетей	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

## 7.2 Примерный перечень оценочных средств (типичные 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. Когда были сформулированы теоретические основы создания компьютерных вирусов?

- (1) в 20-х годах прошлого столетия
- (2) в 40-х годах прошлого столетия**
- (3) в 60-х годах прошлого столетия
- (4) в 80-х годах прошлого столетия

2. Первая глобальная вирусная эпидемия случилась:

- (1) в 1978 году
- (2) в 1986 году**
- (3) в 1991 году
- (4) в 1999 году

3. Вирус – это программа, способная... (продолжите фразу, выбрав наиболее точный вариант)

(1) создавать свои экземпляры (обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению

**(2) создавать свои экземпляры (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению**

(3) нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети

(4) нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

4. Выберите свойство вируса, позволяющее называться ему загрузочным

- (1) способность заражать загрузочные сектора жестких дисков**

- (2) способность вызывать перезагрузку компьютера-жертвы
- (3) способность подсвечивать кнопку Пуск на системном блоке

5. Выберите все типы вирусов, относящиеся к классу файловых вирусов

- (1) загрузочные вирусы
- (2) макровирусы**
- (3) скрипт-вирусы**
- (4) P2P-черви
- (5) логические бомбы

6. Сетевой червь – это ... (продолжите фразу, выбрав наиболее точный вариант)

**(1) вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом**

(2) вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, совпадающих с оригиналом

(3) вредоносная программа, распространяющаяся по сетевым каналам и способная установить на чужом компьютере некую троянскую программу

(4) вредоносная программа, распространяющаяся по сетевым каналам и способная проникнуть на чужой компьютер для выполнения ряда заложенных автором функций. Механизм размножения для сетевых червей не предусмотрен

7. Среди червей выделяют такие типы: (выберите все правильные ответы)

- (1) сетевые**
- (2) файловые
- (3) почтовые**
- (4) скриптовые
- (5) веб-черви
- (6) IM-черви**

8. Среди троянов выделяют такие типы: (выберите все правильные варианты)

- (1) клавиатурные шпионы**
- (2) похитители паролей**
- (3) дефрагментаторы дисков
- (4) утилиты скрытого администрирования**
- (5) логические бомбы**
- (6) шутки
- (7) вирусные мистификации

9. В чем состоит главное отличие трояна от классического вируса или червя?

- (1) в способности к саморазмножению
- (2) в неспособности к саморазмножению**
- (3) в способности к самораспространению с использованием сетевых каналов
- (4) в способности маскировки под легальную программу
- (5) в способности отложить на заданный автором срок выполнение заложенных вредоносных функций

10. К классу условно опасных относятся программы... (выберите наиболее точное определение)

- (1) о которых нельзя однозначно сказать, что они вредоносны**
- (2) последствия выполнения которых нельзя предугадать
- (3) которые можно выполнять только при наличии установленного антивирусного программного обеспечения
- (4) характеризующиеся способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны

### 7.2.2 Примерный перечень заданий для решения стандартных задач

1. Вследствие каких причин на компьютер с установленным современным антивирусным обеспечением могут проникнуть вирусы? Выберите все реальные ситуации

**(1) на момент заражения антивирусная защита была пользователем отключена**

**(2) использовались старые антивирусные базы**

(3) права учетной записи, под которой был выполнен вход в операционную систему, ограничивали возможности антивирусной защиты

**(4) вирус использовал новую, еще не изученную экспертами антивирусной компании технологию**

2. На какие типы принято делить все методы антивирусной защиты?

(1) теоретические

(2) практические

**(3) организационные**

**(4) технические**

(5) программные

3. В каких из перечисленных ситуаций будет полезен брандмауэр (firewall)?

**(1) в борьбе против трояна, ворующего конфиденциальную информацию**

(2) в борьбе против почтовых червей

(3) в защите от фишинга

(4) в защите от спама

4. В чем заключается сигнатурный метод антивирусной проверки? Выберите наиболее точный ответ

(1) в анализе поведения файла в разных условиях

**(2) в сравнении файла с известными образцами вирусов**

(3) в отправке файлов на экспертизу в компанию-производителя антивирусного средства

(4) в анализе кода на предмет наличия подозрительных команд

5. В чем заключается эвристический метод антивирусной проверки?

Выберите все правильные положения

(1) в выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах

**(2) в предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных**

**(3) в анализе поведения файла, а именно контроль за всеми выполняемым им действиями на наличие подозрительных команд**

(4) в отправке файлов на экспертизу в компанию-производителя антивирусного средства

6. Выберите обязательные свойства любого современного антивирусного комплекса?

**(1) не мешать выполнению основных функций компьютера**

(2) не занимать много системных ресурсов

(3) не занимать канал Интернет

**(4) надежно защищать от вирусов**

7. По каким признакам различаются антивирусные комплексы?

**(1) предназначению компьютера/компьютеров (от домашнего до корпоративного)**

(2) опыту пользователя/пользователей (от новичка до профессионала)

**(3) функций, выполняемых компьютером/компьютерами (от домашнего компьютера до почтового сервера или шлюза Интернет)**

(4) степени надежности защиты

8. С какой целью производится деление режимов работы антивируса на проверку в режиме реального времени и проверку по требованию? Выберите наиболее точный ответ

(1) для одновременного использования двух разных методов антивирусного анализа: сигнатурного и эвристического

**(2) для обеспечения одновременной и непрерывной антивирусной защиты, и надежности**

(3) для разграничения пользовательских прав на изменения ряда настроек

(4) во избежание остановки антивирусной защиты во время загрузки новых антивирусных баз

9. В чем состоит главное отличие списков настраиваемых параметров антивирусной проверки по требованию от проверки в режиме реального времени?

(1) в необходимости задать ограничение времени проверки

**(2) в необходимости задать область проверки**

(3) в отсутствии возможности задать расписание запуска проверки

(4) в отсутствии возможности указать не запускать проверку автоматически после загрузки операционной системы

10. Что такое антивирусный комплекс? Выберите наиболее точное определение

(1) набор программ, реализующих два режима антивирусной проверки (в режиме реального времени и по требованию), а также средства для обновления антивирусных баз и управления

(2) набор программ, обеспечивающих антивирусную защиту для группы разнородных компьютеров, в которую могут входить рабочие станции, почтовые сервера, шлюзы Интернет

(3) набор программ, предназначенных для решения практических проблем по обеспечению двух режимов антивирусной проверки, а также содержащий средства для обновления антивирусных баз и управления

**(4) набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем и содержащий средство для обновления антивирусных баз**

### 7.2.3 Примерный перечень заданий для решения прикладных задач

1. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

детектор;+  
доктор;  
сканер;  
ревизор;  
сторож.

2. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

детектор;  
доктор;+  
сканер;  
ревизор;  
сторож.

3. Атака доступа - это:

попытка получения злоумышленником информации, для просмотра которой у него нет разрешений +

попытка неправомерного изменения информации

атака, запрещающая легальному пользователю использование системы, информации или возможностей компьютеров

попытка дать неверную информацию о реальном событии или транзакции

4. Подслушивание - это:

просмотр файлов и документов для поиска информации

получение информации из чужого разговора +

захват информации в процессе ее передачи

5. Какие разновидности атак модификации существуют?

замена +  
удаление +  
добавление +  
перемещение  
копирование

6. Какие этапы реализации большинства угроз безопасности (жизненный цикл угроз), **НЕ** включают в себя следующие процессы:

зарождение;  
развитие;  
проникновение в АС;  
проникновение в критичную информацию;  
инициализация;  
результат действия;  
регенерация.

**выбор способа реализации**

7. Какой вариант не относится к обработке риска:

снижение риска,  
сохранение риска,  
предотвращение риска  
перенос риска

**ликвидация риска**

8. Снижение риска это -....

**действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском**

принятие бремени потерь или выгод от конкретного риска  
задание границ применения менеджмента риска, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ

9. Предотвращение риска это -....

**решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее.**

разделение с другой стороной бремени потерь или выгод от риска  
принятие бремени потерь или выгод от конкретного риска

10. Критерии принятия риска устанавливаются на этапе...

**анализа контекста**

оценивания риска  
коммуникации риска

11. В стандарте NIST 800-30:2002 рассматриваются вопросы \_\_\_\_\_

*Ответ: интеграции управления риском в жизненный цикл развития системы*

#### 7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Сформулируйте понятие уязвимости.
2. Сформулируйте понятие риск-анализа.
3. Что представляет собой процесс оценки рисков?
4. Какими понятиями оперируют при анализе рисков в отношении конкретной системы?
5. По каким критериям можно оценивать риски?
6. Что представляет собой объективная вероятность?
7. Что представляет собой субъективная вероятность?
8. Математическое ожидание случайной величины.
9. Дисперсия случайной величины.
10. Среднеквадратическое отклонение случайной величины.
11. Начальные моменты случайной величины.
12. Центральные моменты случайной величины.
13. Коэффициент асимметрии случайной величины.
14. Коэффициент эксцесса случайной величины.
15. Алгоритм расчета общего риска системы на основе пиковых оценок риска в ее компонентах.

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

Не предусмотрено учебным планом

#### 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>Анализ разновидностей вирусных атак и исследование особенностей распространения вирусных эпидемий.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение файловым вирусом, заражение сетевым вирусом.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата,

			требования к курсовому проекту....
3	<i>Оценка вероятности заражения элементов информационно-телекоммуникационной системы: заражение загрузочным вирусом, макровирусом, скрипт-вирусом.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	<i>Оценка вероятностей реализации различных этапов вирусной атаки.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных систем в условиях распространения эпидемии по модели SI.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SIS.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
7	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SEIS.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
8	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SIR.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
9	<i>Риск-анализ и оценка эпистойкости информационно-телекоммуникационных сетей в условиях распространения вирусной эпидемии по модели SEIR.</i>	ОПК-2, ПК-5	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 методики 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 методики 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 методики выставления оценки при проведении промежуточной аттестации.

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

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

#### *Основная литература*

Радько Н.М. Риск-анализ вирусных атак на информационно-телекоммуникационные системы: учеб. пособие, 2015.

Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа: монография, 2010.

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*

Радько Н.М., Голозубов А.А., Макаров О.Ю. Задача риск-анализа атак «вредоносными» // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 139-140. 2013.

Радько Н.М., Гусев Д.В., Калашников А.О. Риск-анализ и оценка эпистойкости информационно-телекоммуникационной системы в условиях распространения информационной эпидемии по модели SIR // Информация и безопасность. – 2014. – Т. 17. – Вып. 7. – С. 44-49. 2014

Радько Н.М., Гусев Д.В. Оценка эпистойкости информационно-телекоммуникационной системы, в которой развивается информационная эпидемия по модели SIR // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем. – 2014. – Вып. 1. – С. 85-97. 2014.

Радько Н.М., Мошненко Р.Н. Риск-анализ информационной эпидемии в информационно-телекоммуникационных системах, распространяющихся по модели SEIS // Информация и безопасность. – 2014. – Т. 17. – Вып. 7. – С. 126-129. 2014.

#### *Методические разработки*

Радько Н.М. [и др.] Методические указания к практическим занятиям по дисциплине «Риск-анализ вирусных атак на информационно-телекоммуникационные системы» для аспирантов для

аспирантов направления подготовки 10.06.01 «Информационная безопасность» очной формы обучения. 2015

Радько Н.М. [и др.] Методические указания к самостоятельным работам по дисциплине «Риск-анализ вирусных атак на информационно-телекоммуникационные системы» для аспирантов для аспирантов направления подготовки 10.06.01 «Информационная безопасность» очной формы обучения. 2015

**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>

[е](#)

Руководство по методология управления, контроля и аудита информационных систем (COBIT) 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----7sbab7afcqes2bn.xn--p1ai/>

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 «Риск-анализ вирусных атак на информационно-телекоммуникационные системы и сети» читаются лекции.

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

<b>Вид учебных занятий</b>	<b>Деятельность студента</b>
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, 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.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов

	<p>лекций;</p> <ul style="list-style-type: none"> <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 три дня эффективнее всего использовать для повторения и систематизации материала.</p>

