

**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 информационно-телекоммуникационных систем и сетей, подвергающихся флуд-атакам различного вида.

1.2. Задачи освоения дисциплины

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Риск-анализ флуд-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 флуд-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 основные методы риск-анализа успешных реализаций флуд-атак на ИТКС
	уметь применять разработанные методы риск-анализа с целью повышения защищенности ИТКС
ПК-5	знать основные этапы риск-анализа деструктивных информационных воздействий, реализуемых в отношении ИТКС; основные типы флуд-атак, специфику их реализации и оценки рисков
	уметь использовать аппарат риск-анализа для оценки рисков реализации флуд-атак на информационно-телекоммуникационные системы и сети; применять типовые методы риск-анализа флуд-атак в отношении ИТКС различного назначения

	владеть методологией риск-анализа в области управления рисками реализации успешных флуд-атак на информационно-телекоммуникационные системы и сети
--	---

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Риск-анализ флуд-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
Аудиторные занятия (всего)	10	10
В том числе:		
Лекции	10	10
в том числе в форме практической подготовки	4	4
Самостоятельная работа	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>Сущность флуд-атак. Атаки, направленные на приведение жертвы в недоступное состояние. Многофункциональные атаки.</i>	Сравнительный анализ существующих флуд-атак и исследование механизмов их реализации. Исследование механизмов защиты от флуд-атак с учетом специфики атакуемого объекта и возможных средств его защиты.	4	2	8	12
2	<i>Специфика моделирования процесса атаки, использующей вредоносную программу IM-Flooder. Измерение ущерба при реализации атаки типа IM-флуд.</i>	Аналитическое моделирование процесса реализации флуд-атак, реализуемых с использованием вредоносной программы IM-Flooder.	4	2	8	12
3	<i>Оценка рисков при реализации атаки типа IM-флуд. Возможности и рекомендации для регулирования рисков в условиях реализации флуд-атаки с использованием вредоносной программы IM-flooder.</i>	Построение вероятностных риск-моделей реализаций на ИТКС атак типа IM-флуд, учитывающих физические характеристики атаки и атакуемой системы. Исследование методов регулирования риска реализации атак типа IM-флуд, базирующихся на полученных риск-моделях.	4	2	8	12

4	<i>Моделирование процесса атаки типа «простой DNS-flood». Моделирование процесса атаки типа «рекурсивный DNS-flood».</i>	Аналитическое моделирование процесса реализации флуд-атак типа «простой DNS-flood». Аналитическое моделирование процесса реализации флуд-атак типа «рекурсивный DNS-flood».	4	2	8	12
5	<i>Определение функции ущерба при реализации атаки типа DNS-флуд. Аналитическая оценка риска при реализации атаки типа DNS-флуд. Рекомендации для регулирования рисков в условиях флуд-атаки типа «DNS-flooder».</i>	Построение аналитической функции ущерба и вероятностных риск-моделей реализаций на ИТКС атак типа DNS-флуд, учитывающих физические характеристики атаки и атакуемой системы. Исследование методов регулирования риска реализации атак типа DNS-флуд, базирующихся на полученных риск-моделях.	4	2	7	12
6	<i>Особенности моделирования процесса атаки, реализуемой посредством вредоносной программы SMS-Flooder. Моделирование процесса атаки типа «SMS-Flood». Функция ущерба от SMS-флуда.</i>	Аналитическое моделирование процесса реализации флуд-атак, реализуемых с использованием вредоносной программы SMS-Flooder. Аналитическое моделирование функции ущерба при реализации атак типа SMS-флуд на системы различного характера.	4	2	6	12
7	<i>Аналитическая оценка риска при реализации атаки типа «SMS-Flood». Возможности и рекомендации для регулирования рисков в условиях флуд-атаки посредством вредоносной программы SMS-Flooder.</i>	Построение вероятностных риск-моделей реализаций на ИТКС атак типа SMS-флуд, учитывающих физические характеристики атаки и атакуемой системы. Исследование методов регулирования риска реализации атак типа SMS-флуд, базирующихся на полученных риск-моделях.	2	1	6	12
8	<i>Моделирование процесса заражения хоста вредоносной программой Email-flooder. Моделирование флуд-атаки на почтовый сервер. Обоснование функции ущерба от почтового флуда.</i>	Аналитическое моделирование процесса реализации флуд-атак, реализуемых с использованием вредоносной программы Email-Flooder. Аналитическое моделирование функции ущерба при реализации атак типа Email-флуд на системы различного характера.	2	1	6	12
9	<i>Аналитическая оценка рисков почтового флуда. Возможности и рекомендации для регулирования рисков в условиях атаки типа «почтовый флуд».</i>	Построение вероятностных риск-моделей реализаций на ИТКС атак типа Email-флуд, учитывающих физические характеристики атаки и атакуемой системы. Исследование методов регулирования риска реализации атак типа Email-флуд, базирующихся на полученных риск-моделях.	2	1	6	12
Итого			30	15	63	108

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:

	риск-анализа успешных реализаций флуд-атак на ИТКС	риск-анализа успешных реализаций флуд-атак на ИТКС	работ в срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
	уметь применять разработанные методы риск-анализа с целью повышения защищенности ИТКС	умение применять разработанные методы риск-анализа с целью повышения защищенности ИТКС	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать основные этапы риск-анализа деструктивных информационных воздействий, реализуемых в отношении ИТКС; основные типы флуд-атак, специфику их реализации и оценки рисков	знание основных этапов риск-анализа деструктивных информационных воздействий, реализуемых в отношении ИТКС; основные типы флуд-атак, специфику их реализации и оценки рисков	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать аппарат риск-анализа для оценки рисков реализации флуд-атак на информационно-телекоммуникационные системы и сети; применять типовые методы риск-анализа флуд-атак в отношении ИТКС различного назначения	умение использовать аппарат риск-анализа для оценки рисков реализации флуд-атак на информационно-телекоммуникационные системы и сети; применять типовые методы риск-анализа флуд-атак в отношении ИТКС различного назначения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методологией риск-анализа в области управления рисками реализации успешных флуд-атак на информационно-телекоммуникационные системы и сети	владение методологией риск-анализа в области управления рисками реализации успешных флуд-атак на информационно-телекоммуникационные системы и сети	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 основные методы риск-анализа успешных реализаций флуд-атак на ИТКС	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять разработанные методы риск-анализа с целью повышения защищенности ИТКС	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	знать основные этапы риск-анализа деструктивных информационных воздействий, реализуемых в отношении ИТКС; основные типы флуд-атак, специфику их реализации и оценки рисков	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь использовать аппарат риск-анализа для оценки рисков реализации флуд-атак на информационно-телекоммуникационные системы и сети; применять типовые методы риск-анализа флуд-атак в	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

отношении ИТКС различного назначения			
владеть методологией риск-анализа в области управления рисками реализации успешных флуд-атак на информационно-телекоммуникационные системы и сети	Решение прикладных задач в конкретной предметной области	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. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?

- (1) атака
- (2) угроза**
- (3) уязвимость
- (4) слабое место системы

2. Как называется попытка реализации угрозы?

- (1) атака**
- (2) нападение
- (3) уязвимость
- (4) слабое место системы

3. Как называется возможность осуществления угрозы Т в отношении объекта О?

- (1) слабость
- (2) неполнота
- (3) уязвимость**
- (4) риск

4. Выделите утверждение, верное в отношении защиты сетей.

(1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

(2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

(3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

(4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

5. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

- (1) эффективность безопасности
- (2) гарантированность безопасности**
- (3) непрерывность безопасности
- (4) надежность безопасности

6. Злоумышленник послал на атакуемый сервер множество SYN-пакетов и не выслал на SYN-ACK пакеты ответы, в результате чего

сервер потерял способность устанавливать новые соединения с легальными пользователями. Какая атака была реализована?

- (1) анализ сетевого трафика
- (2) подмена доверенного объекта сети
- (3) отказ в обслуживании**
- (4) фишинг

7. К какому типу атак относится UDP-flood и ICMP-flood?

- (1) анализ сетевого трафика
- (2) подмена доверенного объекта сети
- (3) отказ в обслуживании**
- (4) фишинг

8. Переведите на язык Интернета выражение «лить воду»:

- (1) флейм
- (2) флуд**
- (3) СПАМ

9. DoS-атаки чаще всего предпринимаются с использованием

- (1) идентификаторов доступа
- (2) спецификаторов кодогенерационных последовательностей
- (3) фальсификации адреса отправителя**
- (4) SPAM

10. Протоколы, имеющие дефекты, и на которые совершаются атаки:

- (1) TCP**
- (2) SMTP**
- (3) HTTP**
- (4) DNS**

7.2.2 Примерный перечень заданий для решения стандартных задач

1. К классам атак следует отнести

- (1) атаки, базирующиеся на дефектах протоколов**
- (2) атаки, использующие дефекты операционной системы**
- (3) поиск и использование слабых мест программ-приложений**
- (4) атаки, эксплуатирующие человеческие слабости**

2. Атаки классифицируются и распределяются

- (1) по сигнатурам**
- (2) по времени суток**
- (3) по сложности распознавания**
- (4) по методам противодействия**

3. Что такое DNS-флуд?

(1) Это очень масштабные атаки, измеряемые в гигабитах в секунду (Гбит/с) или в пакетах в секунду (PPS)

(2) Это симметричная атака, запущенная множественными зомби, находящимися в бот-сети и относящаяся к классу атак UDP

(3) Это атака прикладного уровня заключается в отправке огромного количества запросов, требующих большой вычислительной мощности

4. К DoS-атакам следует отнести

- (1) SYN-штормы**

- (2) АСК-штормы**
 - (3) широковещательные запросы**
 - (4) ICMP-запросы по широковещательным адресам**
5. Что такое "syn flooding"?
- (1) метод противодействия DoS-атакам
 - (2) способ атаковать протокол TCP**
 - (3) вид атаки на ISDN
 - (4) принцип борьбы с червями
6. Достаточной информацией для атаки DNS извне является
- (1) номер используемого UDP-порта**
 - (2) ISN**
 - (3) пароль входа
 - (4) идентификатор обратной связи
7. Чтобы полностью предотвратить атаку ICMP-flood необходимо:
- (1) отключить ICMP-функциональность целевой системы**
 - (2) перенастроить брандмауэр
 - (3) ограничить скорость обработки входящих пакетов ICMP или ограничить допустимость размера запросов ICMP**
8. Какие программы чаще всего используют спамеры:
- (1) Email-flood**
 - (2) IM-flood**
 - (3) DNS-flood
 - (4) SMS-flood**
9. Как называется атака, при которой злоумышленник генерирует большое количество сообщений с разных источников для почтового сервера, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу?
- (1) UDP-flood
 - (2) ICMP-flood
 - (3) SYN-flood
 - (4) Mailbombing**
10. Расположите этапы флуд-атаки на мобильное устройство с использованием вредоносной программы SMS-flood в правильном порядке:
- 1. атакуемый объект обнаружил атаку и начинает применять средства защиты;
 - 2. атака началась, но успех не достигнут;
 - 3. успех атаки достигнут, атака продолжается;
 - 4. устранение атаки и ее последствий.
- (1) 2,3,1,4**
 - (2) 4,3,1,2
 - (3) 1,3,2,4

7.2.3 Примерный перечень заданий для решения прикладных задач

1. К низкоуровневым атакам относятся:

атаки на сетевом уровне

атаки транспортного уровня

сеансового уровня

канального уровня

2. Атака Smurf или ICMP-флуд это _____

Ответ: Злоумышленник использует широковежательную рассылку для проверки работающих узлов в системе, отправляя ping-запрос. Очевидно, атакующий в одиночку не сможет вывести из строя компьютер-жертву, поэтому требуется ещё один участник — это усиливающая сеть.

3. Атака Fraggle (UDP-флуд) это _____

Ответ: является полным аналогом Smurf-атаки, где вместо ICMP пакетов используются пакеты UDP, поэтому её ещё называют UDP-флуд.

4. Атака с помощью переполнения пакетами SYN (SYN-флуд) это _____

Ответ: одна из разновидностей сетевых атак типа отказ от обслуживания, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок

5. Как подразделяются вирусы в зависимости от деструктивных возможностей?

сетевые, файловые, загрузочные, комбинированные

безвредные, неопасные, опасные, очень опасные

резидентные, нерезидентные

полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

6. HTTP-флуд и ping-флуд это _____

Ответ: Это самый примитивный вид DoS-атаки. Насыщение полосы пропускания можно осуществить с помощью обычных ping-запросов только в том случае, если канал атакующего намного шире канала компьютера-жертвы.

7. IP-спуфинг это _____

Ответ: Вид хакерской атаки, заключающийся в использовании чужого IP-адреса источника с целью обмана системы безопасности.

8. TCP Hijacking это _____

Ответ: Разновидность атаки «Человек посередине», когда атакующий способен просматривать пакеты участников сети и посылать свои собственные пакеты в сеть.

9. Атака TCP Reset это _____

Ответ: способ манипулирования интернет-соединениями. В одних случаях, так действуют злоумышленники, в других — легитимные пользователи

10. Сетевые черви это?

а) являются вредоносными программами, которые могут "размножаться"

и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

б) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

в) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

г) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

д) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. По какой причине флуд-атаки в настоящее время представляют опасность для информации, обрабатываемой в ИТКС?

2. Какие флуд-атаки наиболее актуальны в настоящее время?

3. Сформулируйте понятие атаки.

4. Сформулируйте понятие угрозы.

5. Сформулируйте понятие риска.

6. Сформулируйте понятие защищенности.

7. Сформулируйте понятие ущерба.

8. На какие две группы можно подразделить существующие флуд-атаки?

9. Опишите принцип реализации флуд-атаки типа «DNS-флуд».

10. Опишите принцип реализации флуд-атаки типа «SMS-флуд».

11. Формула дополнительного движения риска.

12. Матрица дифференциальной чувствительности риска.

13. Матрица относительной чувствительности риска.

Методы оценки защищенности атакуемых систем.

14. Дайте определение понятия «флуд».

15. Какую цель могут преследовать флуд-атаки?

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>Сущность флуд-атак. Атаки, направленные на приведение жертвы в недоступное состояние. Многофункциональные атаки.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	<i>Специфика моделирования процесса атаки, использующей вредоносную программу IM-Flooder. Измерение ущерба при реализации атаки типа IM-флуд.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	<i>Оценка рисков при реализации атаки типа IM-флуд. Возможности и рекомендации для регулирования рисков в условиях реализации флуд-атаки с использованием вредоносной программы IM-flooder.</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	<i>Моделирование процесса атаки типа «простой DNS-flood». Моделирование процесса атаки типа «рекурсивный DNS-flood».</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	<i>Определение функции ущерба при реализации атаки типа DNS-флуд. Аналитическая оценка риска при реализации атаки типа DNS-флуд. Рекомендации для регулирования рисков в условиях флуд-атаки типа «DNS-flooder».</i>	ОПК-2, ПК-5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	<i>Особенности моделирования процесса атаки, реализуемой посредством вредоносной программы SMS-Flooder. Модели процесса атаки типа «SMS-Flood». Функция ущерба от SMS-флуда.</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

Борисов В.И., Бурса М.В. Риск-анализ флуд-атак на информационно-телекоммуникационные системы и сети: учебное пособие, 2015.

Борисов В.И., Бурса М.В. Математические основы риск-анализа: учебное пособие, 2013.

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

Дополнительная литература

Язов Ю.К., Бурушкин А.А., Панфилов А.П. Марковские модели процессов реализации сетевых атак типа «отказ в обслуживании» // Информация и безопасность. – 2008, – Т. 14. – Вып. 1. – С.79-84.

Тишков С.А. Риск-модели распределенных атак отказа в обслуживании // Информация и безопасность. – 2008. – Т. 11. – Вып. 4. – С. 613–614.

Радько Н.М. Сети Петри в описании атак на информационно-телекоммуникационные системы // Информация и безопасность. – 2007. – Т. 10. – Вып. 2. – С. 362-364. Радько Н.М.,

Скобелев И.О., Плотников Д.Г. К вопросу о выборе мер защиты для различных типов информационно-телекоммуникационных систем // Информация и безопасность. – 2010. – Т. 13. – Вып. 1. – С. 55-65 2010

Методические разработки

А.Г. Остапенко, В.В. Бутузов, М.В. Бурса, А.О. Калашников, Г.А. Остапенко Методические указания к практическим занятиям по дисциплине «Риск-анализ флуд-атак на информационно-телекоммуникационные системы и сети» для аспирантов для аспирантов направления подготовки 10.06.01 «Информационная безопасность» очной формы обучения, 2015.

А.Г. Остапенко, В.В. Бутузов, М.В. Бурса, А.О. Калашников, Г.А. Остапенко Методические указания самостоятельным работам по дисциплине «Риск-анализ флуд-атак на информационно-телекоммуникационные системы

и сети» 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

Сборник программ по риск-менеджменту

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

e

Руководство по методологии 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 «Риск-анализ флуд-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.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить 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: <ul style="list-style-type: none">- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;- выполнение домашних заданий и расчетов;- работа над темами для самостоятельного изучения;- участие в работе студенческих научных конференций, олимпиад;- подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	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.

