

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета ФИТКБ
/Гусев П.Ю./
28.02.2023 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Операции и атаки в компьютерных системах и сетях»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы
Заведующий кафедрой
Систем информационной
безопасности

А.Е. Дешина

А.Г. Остапенко

К.А. Разинкин

Руководитель ОПОП

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является приобретение студентами знаний о структуре действий, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

1.2. Задачи освоения дисциплины

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области формализация описания информационных конфликтов социотехнических систем, стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах. Стратегии реализации информационных операций и атак;

- предоставить возможность изучения технологии поиска и анализа следов информационных операций и атак и инцидентов, прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Операции и атаки в компьютерных системах и сетях» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Операции и атаки в компьютерных системах и сетях» направлен на формирование следующих компетенций:

ПК-4.4 - Способен участвовать в работах по проведению экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.4	Знать нормативные правовые акты в области защиты информации, регулирующие расследование компьютерных преступлений и инцидентов
	Уметь определять характеристики аппаратных средств, операционных систем и технологий системного программирования в исследуемых компьютерных системах, анализировать функциональные свойства и алгоритмы программного обеспечения, выявлять недокументированные возможности.
	Владеть навыками определения механизма, динамики и обстоятельств события по имеющимся цифровым следам, методиками установления участников инцидента, их роли,

места и условий, при которых была создана, модифицирована или удалена информация.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Операции и атаки в компьютерных системах и сетях» составляет 12 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	180	72	108
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	108	36	72
Самостоятельная работа	216	36	180
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет с оценкой	+	+	+
Общая трудоемкость:			
академические часы	432	108	324
зач.ед.	12	3	9

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	Лаб. зан.	СРС	Всего, час
1	Введение. Классификация атак	Классификация атак как основа для идентификации инцидентов при расследовании. Виды атак по характеру, цели, расположению субъекта, уровню модели OSI. Анализ принадлежности атаки к конкретному типу для определения методов расследования. Примеры из практики компьютерной криминалистики.	12	18	36	66
2	Этапы реализации атак	Анализ этапов атаки (сбор информации, сканирование, проникновение, закрепление) с позиции эксперта. Выявление цифровых следов на каждом этапе: логи сканирования, артефакты внедрения, журналы системы. Восстановление хронологии действий нарушителя по цифровым следам.	12	18	36	66
3	Краткое описание некоторых сетевых атак	Анализ этапов атаки (сбор информации, сканирование, проникновение, закрепление) с позиции эксперта. Выявление цифровых следов на каждом этапе: логи сканирования, артефакты внедрения, журналы системы. Восстановление хронологии действий нарушителя по цифровым следам. ложного	12	18	36	66

		маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки):SYN-flood,UDP-flood				
4	Технологии обнаружения атак	Применение систем обнаружения вторжений (IDS), статистических методов и нейронных сетей для выявления инцидентов. Анализ срабатываний IDS как источник доказательств. Использование SIEM-систем для сбора и корреляции событий безопасности при расследовании.	12	18	36	66
5	Социальная инженерия	Фишинг и методы социальной инженерии как объект расследования. Анализ фишинговых писем, поддельных сайтов, телефонных звонков. Сбор цифровых следов (заголовки писем, логи DNS, метаданные файлов) для установления источника атаки.	12	18	36	66
6	Проблемы и перспективы применения кибернетического оружия в современной сетцентрической войне	Расследование инцидентов, связанных с применением кибероружия в рамках сетцентрических войн. Анализ атак на критическую инфраструктуру (АСУ ТП). Особенности сбора доказательств в условиях противодействия. Прогнозирование новых видов компьютерных преступлений и методов их расследования.	12	18	36	66
Итого			72	108	216	396

5.2 Перечень лабораторных работ

1.Оценка степени поражения информационным оружием при мониторинге сетевого пространства на предмет выявления информационных операций.

2.Оценка эффективности перепрограммирования субъектов информационного воздействия при мониторинге сетевого пространства на предмет выявления информационных операций.

3.Математическая модель распространения слухов и понятие «реальное время» информационной операции.

4. Формальная постановка задачи на формирование плана информационной операции

5. Планирование информационной операции

6. Моделирование информационной операции

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Стресс-тест сети (DoS веб-сайта) со SlowHTTPTest в Kali Linux»

Задачи, решаемые при выполнении курсового проекта:

- знакомство со имитационными средами атак;
- прогнозирование исходов атак и выработка механизмов защиты;

- знакомство с УК РФ Глава 28 и анализ следов компьютерных преступлений, правонарушений и инцидентов.

Курсовой проект включают в себя графическую часть и расчетно-пояснительную записку.

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
ПК-4.4	Знать нормативные правовые акты в области защиты информации, регулирующие расследование компьютерных преступлений и инцидентов	Демонстрирует знание основных положений УК РФ Глава 28, ФЗ «О безопасности», ФЗ «Об информации...». Ориентируется в нормативной базе, регулирующей порядок расследования инцидентов. Воспроизводит классификацию компьютерных преступлений и правонарушений.	Выполнение лабораторных работ и тестов в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ и тестов в срок, предусмотренный в рабочих программах
	Уметь определять характеристики аппаратных средств, операционных систем и технологий системного программирования в исследуемых компьютерных системах, анализировать функциональные свойства и алгоритмы программного обеспечения, выявлять недокументированные возможности.	Анализирует конфигурацию аппаратных средств и ОС исследуемой системы. Применяет инструменты для анализа программного обеспечения (дизассемблеры, отладчики). Выявляет признаки недокументированных возможностей и аномалий в работе ПО.	Выполнение лабораторных работ и тестов в срок, предусмотренный в рабочих программах	Невыполнение лабораторных работ и тестов в срок, предусмотренный в рабочих программах
	Владеть навыками определения механизма, динамики и обстоятельств	Реконструирует хронологию событий инцидента на основе анализа цифровых следов (логи, дампы, метаданные).	Выполнение лабораторных работ и тестов в срок, предусмотренный	Невыполнение лабораторных работ и тестов в срок, предусмотренный

	события по имеющимся цифровым следам, методиками установления участников инцидента, их роли, места и условий, при которых была создана, модифицирована или удалена информация.	Устанавливает возможные роли участников и последовательность их действий. Определяет условия и обстоятельства, способствовавшие возникновению инцидента.	ый в рабочих программах	ый в рабочих программах
--	--	--	-------------------------	-------------------------

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-4.4	Знать нормативные правовые акты в области защиты информации, регулирующие расследование компьютерных преступлений и инцидентов	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	Уметь определять характеристики аппаратных средств, операционных систем и технологий системного программирования в исследуемых компьютерных системах, анализировать функциональные свойства и алгоритмы программного обеспечения, выявлять недокументированные возможности.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продemonстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продemonстрирован верный ход решения в большинстве задач	Задачи не решены

Владеть навыками определения механизма, динамики и обстоятельств события по имеющимся цифровым следам, методиками установления участников инцидента, их роли, места и условий, при которых была создана, модифицирована или удалена информация.	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 такое DDoS-атака?

Ответ:

- (1) атака с применением методов социальной инженерии
- (2) распределенная атака типа «анализ сетевого трафика»
- (3) распределенная атака типа «отказ в обслуживании»
- (4) распределенная атака типа «подмена доверенного объекта сети»

2) Какие службы безопасности предназначены для защиты от атак доступа?

Ответ:

- (1) конфиденциальность
- (2) целостность
- (3) доступность
- (4) идентифицируемость

3) Какие службы безопасности предназначены для защиты от атак модификации?

Ответ:

- (1) конфиденциальность
- (2) целостность
- (3) доступность
- (4) идентифицируемость

4) Какое свойство службы безопасности предназначены для защиты от атак отказа в обслуживании?

Ответ:

- (1) конфиденциальность
- (2) целостность
- (3) доступность
- (4) идентифицируемость

5) Какие службы безопасности предназначаются для защиты от атак отказ от обязательств?

Ответ:

- (1) конфиденциальность
- (2) целостность
- (3) доступность
- (4) идентифицируемость

6) Для защиты от атак какого типа предназначена служба конфиденциальности?

Ответ:

- (1) атаки доступа
- (2) атаки модификации
- (3) атаки отказа в обслуживании
- (4) атаки отказа от обязательств

7) Для защиты от атак какого типа предназначена служба целостности?

Ответ:

- (1) атаки доступа
- (2) атаки модификации
- (3) атаки отказа в обслуживании
- (4) атаки отказа от обязательств

8) Для защиты от атак какого типа предназначена служба доступности?

Ответ:

- (1) атаки доступа
- (2) атаки модификации
- (3) атаки отказа в обслуживании
- (4) атаки отказа от обязательств

9) Для защиты от атак какого типа предназначена служба идентифицируемости?

Ответ:

- (1) атаки доступа
- (2) атаки модификации
- (3) атаки отказа в обслуживании
- (4) атаки отказа от обязательств

10) К механизмам физической безопасности относятся:

Ответ:

- (1) контроль физической безопасности
- (2) правильная настройка компьютерной системы
- (3) правильное управление ключами при использовании шифрования

7.2.2 Примерный перечень заданий для решения стандартных задач

1) DoS-атаки чаще всего предпринимаются с использованием

Ответ:

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

2) Модификация сигнатуры без изменения сущности атаки лежит в основе

Ответ:

- (1) SPAM
- (2) сетевых вирусов
- (3) детекторов
- (4) каунтеров

3) Методы атак против протокола TCP

Ответ:

(1) атака возможна только в случае, если атакующая машина находится на пути от клиента к серверу

(2) возможна атака за счет сбоя ISN-нумерации пакетов
(3) возможна атака с помощью фальсификации CRC
(4) атаки на TCP-уровне невозможны. Если бы это было не так, стали бы возможны атаки практически на любые процедуры Интернет, ведь практически все они базируются на протоколе TCP

4) Что такое атака переполнения буфера?

Ответ:

(1) это попытка ввести в HTML-форму больше символов, чем для этого выделено
(2) это попытка переполнить любой программный буфер при вводе символов с клавиатуры
(3) это попытка ввести вместе с текстом какой-то вредоносный код
(4) это попытка передать через сеть более длинное сообщение, чем было запрошено

5) Что происходит при атаках на CGI?

Ответ:

(1) генерация нестандартных строк URL
(2) сбой доступа к серверу DNS
(3) применение метода прямой осцилляции к системным кодам
(4) поражение BIOS

6) В основе атак протокола HTTP лежит

Ответ:

(1) фальсификация методов и заголовков объектов
(2) сбой доступа к стандартным URL
(3) блокировка параметров конфигурации
(4) блокировка доступа к инициализирующим приложениям

7) Что такое "syn flooding"?

Ответ:

(1) метод противодействия DoS-атакам
(2) способ атаковать протокол TCP
(3) вид атаки на ISDN
(4) принцип борьбы с червями

8) Достаточной информацией для атаки DNS извне является

Ответ:

- (1) номер используемого UDP-порта
- (2) ISN
- (3) пароль входа
- (4) идентификатор обратной связи

9) Атаки классифицируются и распределяются

Ответ:

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

10) Атаки, сопряженные с манипуляциями при обмене сообщениями и фальсификациями заголовков, производятся на протоколы типа

Ответ:

- (1) SMTP
- (2) IMAP
- (3) POP3
- (4) NNTP

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Как называется атака, заключающаяся в прослушивании канала связи с использованием специального программно-аппаратного устройства или программы-анализатора пакетов?

Ответ:

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

2) На каком уровне модели OSI реализуется атака типа «анализ сетевого трафика»?

Ответ:

- (1) сетевой
- (2) канальный
- (3) транспортный

(4) прикладной

- 3) На каких уровнях модели OSI реализуется атака «Отказ в обслуживании»?

Ответ:

- (1) сетевой
- (2) канальный
- (3) транспортный
- (4) прикладной

- 4) 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?

Ответ:

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

- 5) К какому типу атак относится UDP-flood и ICMP-flood?

Ответ:

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

- 6) 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?

Ответ:

- (1) UDP-flood
- (2) ICMP-flood
- (3) SYN-flood
- (4) Mailbombing

- 7) Николай получил поддельное письмо от электронной платежной системы с просьбой проверить последние платежи. Ссылка в письме вела сайт, похожий на официальный сайт платежной системы. Какой атаке подвергся Николай?

Ответ:

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

- 8) Какое требование к системе защиты информации предполагает то, что методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления?

Ответ:

- (1) адекватность
- (2) непрерывность
- (3) централизованность
- (4) универсальность

- 9) Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

Ответ:

- (1) адекватность
- (2) непрерывность
- (3) централизованность
- (4) универсальность

- 10) Для чего применяется экранирование помещений и дополнительное заземление объектов защиты?

Ответ:

- (1) для увеличения уровня побочных электромагнитных излучений
- (2) для уменьшения уровня побочных электромагнитных излучений
- (3) для обеспечения бесперебойного питания объектов защиты
- (4) для исключения внедрения злоумышленников во внутренние сегменты сети

7.2.4 Примерный перечень вопросов для подготовки к зачету с оценкой

1. Приведите классификацию компьютерных атак по характеру воздействия, цели и расположению субъекта атаки. Как знание классификации помогает при расследовании инцидентов?

2. Опишите классификацию атак по уровням модели OSI. Приведите примеры атак для каждого уровня с пояснением, какие цифровые следы остаются на каждом уровне.

3. Какие методы идентификации типа атаки используются в компьютерной криминалистике? Приведите примеры из практики расследований.

4. Перечислите и охарактеризуйте основные этапы подготовки и реализации атаки с позиции эксперта-криминалиста.

5. Какие цифровые следы остаются на этапе сбора информации и сканирования сети? Как их обнаружить и зафиксировать?

6. Опишите процесс восстановления хронологии действий нарушителя по журналам системы и логам сетевого оборудования.

7. Какие артефакты внедрения и закрепления в системе оставляет злоумышленник? Где их искать при расследовании?

8. Опишите механизм спуфинг-атак (IP-спуфинг, DNS-спуфинг). Какие доказательства необходимо собрать для расследования таких атак?

9. Что такое сниффинг (прослушивание канала)? Какие методы применяются для обнаружения факта перехвата трафика и сбора доказательств?

10. Охарактеризуйте DoS и DDoS-атаки (SYN-flood, UDP-flood). Какие данные необходимо сохранить для последующего анализа и установления источника атаки?

11. Какие методы фиксации и документирования сетевых атак используются при проведении экспертизы?

12. Как работают системы обнаружения вторжений (IDS)? Каким образом результаты их работы могут быть использованы в качестве доказательной базы?

13. Опишите применение SIEM-систем для сбора и корреляции событий безопасности при расследовании инцидентов.

14. Какие статистические методы и методы машинного обучения применяются для выявления аномалий и расследования компьютерных атак?

15. Что такое фишинг и какие его разновидности существуют? Опишите методику расследования фишинговых атак.

16. Какие цифровые следы оставляют атаки с использованием методов социальной инженерии (анализ заголовков писем, метаданных файлов, DNS-логов)?

17. Как установить источник фишинговой атаки и собрать доказательства для правоохранительных органов?

18. Какие особенности имеет расследование инцидентов, связанных с применением кибероружия против критической инфраструктуры (АСУ ТП)?

19. Охарактеризуйте проблемы сбора и фиксации доказательств в условиях активного противодействия со стороны злоумышленников.

20. Какие новые виды компьютерных преступлений прогнозируются в ближайшем будущем и какие методы их расследования необходимо разрабатывать?

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Классификация атак по характеру воздействия на атакуемую систему.

2. Классификация атак по цели воздействия.

3. Классификация атак по наличию обратной связи с атакуемым объектом.

4. Классификация атак по условию начала осуществления воздействия.

5. Классификация атак по расположению субъекта атаки относительно атакуемого объекта.

6. Классификация атак по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие.

7. Примеры различных типов атак.

8. Сбор информации: изучение окружения атакуемой системы.

9. Идентификация топологии сети.

10. Идентификация узлов сети.

11. Идентификация сервисов и сканирование портов.

12. Идентификация операционной системы удаленного узла.

13. Определение роли узла в сети.

14. Определение уязвимостей узла.

15. Реализация атаки.

16. Проникновение в систему.

17. Установление контроля над системой.

18. Завершение атаки и сокрытие следов.

20. Атаки, основанные на фрагментации данных.

21. Атака Ping flooding.

22. Использование нестандартных протоколов, инкапсулированных в IP.

23. Атака Smurf.

24. Атака DNS spoofing (подмена DNS).

25. Атака IP spoofing (подмена IP-адреса).

26. Навязывание пакетов.

27. Sniffing — прослушивание канала связи.

28. Перехват пакетов на маршрутизаторе.

29. Навязывание хосту ложного маршрута с помощью протокола ICMP.

30. Атака WinNuke.

32. Подмена доверенного хоста.

32. Отказ в обслуживании (DoS и DDoS-атаки): SYN-flood, UDP-flood.

33. Методы анализа сетевой информации.

34. Статистический метод обнаружения атак.

35. Экспертные системы в обнаружении вторжений.
36. Применение нейронных сетей для обнаружения атак.
37. Несуществующие ссылки.
38. Мошенничество с использованием брендов известных корпораций.
39. Подложные лотереи.
40. Ложные антивирусы и программы для обеспечения безопасности.
41. IVR или телефонный фишинг.
42. Сбор информации из открытых источников:
43. Обратная социальная инженерия.
44. Классификация угроз социальной инженерии:
45. Концепция «сетевых войн».
46. Наступательные операции в киберпространстве как составная часть информационной войны.
47. Наступательные операции против АСУ инфраструктурных и технологических объектов.
48. Оборонительные операции как часть мер по обеспечению информационной безопасности в мирное время.
49. Перспективы развития концепции кибернетических операций.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет с оценкой проводится в виде итогового тестирования, которое включает:

- 10 теоретических вопросов (проверка компонента «знать»);
- 5 стандартных задач (проверка компонента «уметь»);
- 5 прикладных задач (проверка компонента «владеть»).

Распределение баллов

Элемент контроля	Количество заданий	Балл за одно задание	Максимальный балл
Теоретические вопросы	10	1	10 баллов
Стандартные задачи	5	2	10 баллов
Прикладные задачи	5	2	10 баллов
Итого	20		30 баллов

Шкала оценивания

Сумма баллов	Оценка	Уровень освоения компетенции
25–30 баллов ($\geq 83\%$)	«Отлично»	Повышенный уровень
19–24 балла (63–82%)	«Хорошо»	Базовый уровень
13–18 баллов (43–62%)	«Удовлетворительно»	Пороговый уровень
12 баллов и менее (< 43%)	«Неудовлетворительно»	Компетенция не сформирована

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение. Классификация атак	ПК-4.4	Тест, защита лабораторных работ
2	Этапы реализации атак	ПК-4.4	Тест, защита лабораторных работ
3	Краткое описание некоторых сетевых атак	ПК-4.4	Тест, защита лабораторных работ
4	Технологии обнаружения атак	ПК-4.4	Тест, защита лабораторных работ
5	Социальная инженерия	ПК-4.4	Тест, защита лабораторных работ
6	Проблемы и перспективы применения кибернетического оружия в современной сетцентрической войне	ПК-4.4	Тест, защита лабораторных работ

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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Алешкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алешкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167600>

Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/156494>

Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/101992.html>

Дополнительная литература

Белоус, А. И. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия : в 2 книгах / А. И. Белоус, В. А. Солодуха, С. В. Шведов ; под редакцией А. И. Белоуса. — Москва : Техносфера, 2019 — Книга 1 — 2019. — 688 с. — ISBN 978-5-94836-524-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/140565>

Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163932>

Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163812>

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:

База данных уязвимостей (CVE) <https://cve.mitre.org/>

Национальная база данных уязвимостей (NVD) <https://nvd.nist.gov/>

Банк данных угроз безопасности информации (ФСТЭК России) <https://bdu.fstec.ru/>

OWASP Foundation <https://owasp.org/>

Exploit Database <https://www.exploit-db.com/>
Linux manual pages <https://man7.org/linux/man-pages/>
Электронно-библиотечная система «Лань» <https://e.lanbook.com/>
Электронно-библиотечная система IPRbooks <https://iprbookshop.ru/>
http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/ УК РФ Глава 28. Преступления в сфере компьютерной информации.
<https://www.kali.org/> Kali Linux

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой
Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

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

По дисциплине «Операции и атаки в компьютерных системах и сетях» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать 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.

Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомиться с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - 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 с оценкой, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]

