

**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

**«Непосредственно и удаленно атакуемые компьютерные системы и
сети»**

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

Руководитель ОПОП

К.А. Разинкин

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины приобретение будущими специалистами знаний и умений в части анализа угроз в отношении непосредственно и удаленно атакуемых информационной безопасности в компьютерных систем и сетей, участия в работах по управлению рисками систем защиты компьютерных систем и сетей от НСД.

1.2. Задачи освоения дисциплины

- сформировать у будущего специалиста в области безопасности компьютерных систем и сетей знаний относительно классификации и этапов реализации атак, технологии обнаружения атак, в том числе в аспекте социальной инженерии;

- предоставить возможность изучения особенностей, проблем и перспектив применения кибернетического оружия в современной сетевцентрической войне

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Непосредственно и удаленно атакуемые компьютерные системы и сети» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Непосредственно и удаленно атакуемые компьютерные системы и сети» направлен на формирование следующих компетенций:

ПК-4.5 - Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.5	Знать классификацию уязвимостей ПО, аппаратных платформ и сетевых протоколов (CWE, OWASP Top 10), методологию анализа защищенности для локальных и удаленных систем, а также использование современных источников угроз (БДУ ФСТЭК, CVE, NVD).
	Уметь разворачивать и настраивать инструментальные средства для анализа защищенности, проводить сканирование компьютерных сетей и систем для выявления открытых портов, сервисов и их уязвимостей, анализировать сетевой трафик с целью выявления аномалий и признаков проведения атак.
	Владеть навыками анализа механизмов реализации типовых атак, методиками реконструкции последовательности действий нарушителя по цифровым следам (логи, дампы трафика, журналы систем), способностью выявлять причины и условия, способствовавшие успешной реализации атаки, и формулировать рекомендации по устранению выявленных уязвимостей.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Непосредственно и удаленно атакуемые компьютерные системы и сети» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	18	18
Самостоятельная работа	126	126
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы	180	180
зач.ед.	5	5

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	Классификацию уязвимостей ПО, аппаратных платформ и сетевых протоколов (CWE, OWASP Top 10), методологию анализа защищенности для локальных и удаленных систем, а также использование современных источников угроз (БДУ ФСТЭК, CVE, NVD) Классификация по характеру воздействия; по цели воздействия; по наличию обратной связи с атакуемым объектом; по условию начала осуществления воздействия; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Примеры.	6	4	20	30
2	Этапы реализации атак	сбор информации: изучение окружения; идентификация топологии сети; идентификация узлов; идентификация сервисов и сканирование портов; идентификация операционной системы; определение роли узла; определение уязвимостей узла; реализация атаки; проникновение; установление контроля; завершение атаки	6	4	20	30
3	Краткое описание некоторых сетевых атак	фрагментация данных; атака Ping flooding; нестандартные протоколы, инкапсулированные в IP; атака smurf; атака DNS spoofing; атака IP spoofing; навязывание пакетов; Sniffing — прослушивание канала; перехват пакетов на маршрутизаторе;	6	4	20	30

		навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки): SYN-flood, UDP-flood				
4	Технологии обнаружения атак	методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети	6	2	22	30
5	Социальная инженерия	Популярные фишинговые схемы: несуществующие ссылки; мошенничество с использованием брендов известных корпораций; подложные лотереи; ложные антивирусы и программы для обеспечения безопасности; IVR или телефонный фишинг. Сбор информации из открытых источников: плечевой серфинг; обратная социальная инженерия. Способы защиты от социальной инженерии. Классификация угроз: угрозы, связанные с телефоном; угрозы, связанные с электронной почтой; угрозы, связанные с использованием службы мгновенного обмена сообщениями. Основные защитные методы	6	2	22	30
6	Проблемы и перспективы применения кибернетического оружия в современной сетевцентрической войне	Концепция «сетевцентрических войн». Наступательные операции в киберпространстве как составная часть информационной войны. Наступательные операции против АСУ инфраструктурных и технологических объектов. Оборонительные операции как часть мер по обеспечению информационной безопасности в мирное время. Перспективы развития концепции кибернетических операций	6	2	22	30
Итого			36	18	126	180

5.2 Перечень лабораторных работ

1. DDoS основные особенности их организации и защиты. Медленная атака. SlowLoris
2. DDoS основные особенности их организации и защиты. Медленная атака. Slow HTTP POST/GET.
3. DDoS основные особенности их организации и защиты. Медленная атака. Sockstress.
4. DDoS основные особенности их организации и защиты. Атака произвольными пакетами. HTTP-Flood
5. DDoS основные особенности их организации и защиты. Атака произвольными пакетами. SYN-Flood.
6. Атака с помощью SSL
7. Атака почтового сервера. SMTP-Flood
8. Изучение Security information and event management - систем

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
ПК-4.5	Знать классификацию уязвимостей ПО, аппаратных платформ и сетевых протоколов (CWE, OWASP Top 10), методологию анализа защищенности для локальных и удаленных систем, а также использование современных источников угроз (БДУ ФСТЭК, CVE, NVD).	Корректно воспроизводит классификацию атак по различным признакам. Ориентируется в современных базах данных уязвимостей. Демонстрирует понимание методологии анализа защищенности на разных этапах (сбор информации, сканирование, анализ уязвимостей).	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разворачивать и настраивать инструментальные средства для анализа защищенности, проводить сканирование компьютерных сетей и систем для выявления открытых портов, сервисов и их уязвимостей, анализировать сетевой трафик с целью выявления аномалий и признаков проведения атак.	Самостоятельно разворачивает и настраивает программные средства для анализа защищенности. Проводит сканирование сети, идентифицирует открытые порты и сервисы. Анализирует сетевой трафик, выявляет аномалии и признаки атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками анализа механизмов реализации типовых атак, методиками реконструкции последовательности действий нарушителя по цифровым следам (логи,	Воспроизводит типовые атаки в лабораторной среде и анализирует механизмы их реализации. Реконструирует последовательность действий нарушителя на	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

дампы трафика, журналы систем), способностью выявлять причины и условия, способствовавшие успешной реализации атаки, и формулировать рекомендации по устранению выявленных уязвимостей.	основе анализа логов и дампов трафика. Выявляет причины успешной реализации атаки		
---	---	--	--

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 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-4.5	знать методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь использовать приемы защиты от типичных атак на компьютерные системы	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	знание виды атак и механизмы их реализации в компьютерных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	владеть навыками разработки программно-аппаратных средств защиты информации в компьютерных системах	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. Атаки, влияющие на доступность и надежность сайта, называются:
Denial of Service
атаками на отказ в обслуживании
DoS
DsO
Down Service
2. Действия, нарушающие функционирование части автоматизированной информационной системы в соответствии с определенной целью - это:
отказ в обслуживании
хакерство
крекинг
социальный инжиниринг
3. Несанкционированное использование, попытки обмана или обхода систем безопасности компьютерной информационной системы или сети - это:
Hacking
Denial of Service
Cracking
Engineering
4. Акт проникновения в компьютерную систему или сеть - это:
социальный инжиниринг
физическая атака
крекинг
хакерство
5. Термин, описывающий данный тип атаки, он основан на управлении личностью человека для достижения своей цели:
Cracking
Hacking
Denial of Service
Physical attack
Social engineering
6. Эффективной DoS-атакой является:
отсоединение источника питания системы
получение конфиденциальных данных от пользователей под видом службы технической поддержки
разрыв линий коммуникации
7. Сущность защиты от социальных и физических атак заключается в следующем:
размещение компьютеров в безопасных местах
использование камер видеонаблюдения
обучение пользователей
разработка политики безопасности

8. Какая из задач обеспечения безопасности предполагает создание защитных процедур и защищенной веб-среды:

- обнаружение
- реагирование
- предотвращение
- обеспечение

9. Перегрузку сетевых экранов или серверов для замедления их работы или полной остановки из-за обработки огромного количества информации предполагает следующий тип атаки:

- Флудинг узлов, маршрутизаторов или сетевых экранов
- Сниффинг
- Спуфинг
- Взлом таблиц маршрутизаторов
- Маскарад

10. Разновидность подмены пользователя, основанная на имитации его поведения - это:

- захват
- сниффинг
- аннулирование транзакции
- флудинг

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Выберите верные утверждения. При использовании IDS

Возрастает возможность определения преамбулы атаки.

Возрастает возможность фильтрации трафика.

Возрастает возможность определения оптимального маршрута для каждого кадра.

Возрастает возможность раскрытия осуществленной атаки.

2. IDS могут быть реализованы

Только программно.

Только аппаратно.

Только совместно с межсетевым экраном.

Как программно, так и аппаратно.

3. Причины, по которым необходимо использовать IDS

Во многих наследуемых системах не могут быть выполнены все необходимые обновления и модификации.

Даже в системах, в которых обновления могут быть выполнены, администраторы иногда не имеют достаточно времени или ресурсов для отслеживания и инсталлирования всех необходимых изменений.

При конфигурировании системных механизмов управления доступом для реализации конкретной политики всегда могут существовать определенные несоответствия.

При использовании IDS нет необходимости в межсетевых экранах.

4. Преимущества использования IDS

Возможность иметь реакцию на атаку.
Возможность блокирования атаки.
Выполнение документирования существующих угроз для сети и систем.

Нет необходимости в межсетевых экранах.

5. К атакам на содержимое и информацию можно отнести:

повреждение отображаемого на веб-сайте содержимого

нарушение конфиденциальности

удаление файлов

мошенничество

6. Они защищают внутренние ресурсы, маскируя реальные IP-адреса компьютеров и блокируя попытки доступа к сети, инициированные извне, если только внешний пользователь не является законным и авторизованным сотрудником организации:

сетевые экраны

firewalls

брандмауэры

маршрутизаторы

7. При универсальном подходе хакер начинает атаку:

с выполнения тестового опроса (ping)

с осуществления сканирования для обнаружения на атакуемом компьютере доступных служб

с использования крекинга для проникновения в систему

с выполнения атаки на переполнение буфера

8. Атаки направленные не на конкретную организацию, а на большое число потенциальных жертв - это:

атаки широкого диапазона действия

универсальные атаки

атаки узкого диапазона действия

9. Универсальный инструмент хакера, имеющий целью сканирование сети для определения доступных систем и служб, используемых операционных систем называется:

Winscan

LC3 (LOphtcrack)

Nmap

Nessus

Ethereal

Whois

10. К методологии хакерства можно отнести:

случайный поиск или разведка для определения жертв

сбор базовых сведений

создание перечня параметров

выполнение эксплоита

сокрытие действий

зондирование

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Какие серверные службы будут отключены после установки ISA Server?
ICS
ICF
NAT
2. Из приведенных ниже записей выделите серверные службы, которые будут отключены после установки ISA Server:
SNMP
FTP
TTP
3. В зависимости от стратегии внедрения ISA Server существуют сценарии развертывания
для рабочей группы
для сетевых экранов
для службы каталогов Active Directory
4. Сервер, выполняющий роль хранения конфигурации ISA Server, носит название
CSS
ISP
IPC
5. Сервер, выполняющий роль хранения конфигурации ISA Server, носит название
CSS
ISP
IPC
6. Для централизованной аутентификации можно использовать
RADIUS
RETAIL
CONNECT
7. К схемам административных ролей следует отнести
администраторов предприятия
администраторов массива
администраторов блока
8. Из приведенных ниже записей выделите клиентов ISA Server:
Web-прокси
протокол IP
модуль балансировки сети
9. Какие из приведенных ниже записей соответствуют клиентам ISA Server?
DetectIPA
SecureNAT
ModuleDPT

10. Если нужна простая маршрутизация без аутентификации и контроля над действиями пользователей, то нужно применять клиент

ISPDData

SecureNAT

NetScan

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Приведите классификацию компьютерных атак по характеру воздействия на атакуемую систему. Проиллюстрируйте примерами.

2. Какие существуют признаки классификации атак по цели воздействия? Опишите основные типы атак в зависимости от цели.

3. Раскройте классификацию атак по расположению субъекта атаки относительно атакуемого объекта. В чем отличие удаленных и локальных атак?

4. Опишите классификацию атак по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Приведите примеры атак для каждого уровня.

6. Перечислите и охарактеризуйте основные этапы сбора информации об атакуемой системе на предварительной стадии атаки.

7. Какие методы используются для идентификации топологии сети и идентификации узлов? Назовите инструменты, применяемые для этих целей.

8. Опишите процесс сканирования портов. Какие типы сканирования существуют и какова их цель?

9. Какими способами можно идентифицировать операционную систему удаленного узла? На чем основаны эти методы?

10. Перечислите этапы реализации атаки от проникновения до установления контроля над системой. Что понимается под «завершением атаки»?

11. Что такое спуфинг-атаки? Опишите механизм реализации IP-спуфинга и DNS-спуфинга. Каковы цели этих атак?

12. Раскройте понятие «сниффинг» (прослушивание канала). Каким образом осуществляется перехват пакетов и анализ трафика?

13. Опишите атаки, связанные с навязыванием хосту ложного маршрута. Какие протоколы могут быть использованы для реализации таких атак?

14. Дайте характеристику DoS и DDoS-атакам. В чем заключается принцип действия SYN-флуд и UDP-флуд атак?

15. Что такое фрагментация данных и как она может использоваться для реализации атак?

16. Какие существуют методы анализа сетевой информации для обнаружения атак? Охарактеризуйте статистический метод.

17. Опишите принцип работы систем обнаружения вторжений (IDS), основанных на экспертных системах.

18. Каким образом нейронные сети могут применяться для обнаружения компьютерных атак? В чем преимущества и недостатки этого подхода?

19. Что такое социальная инженерия? Опишите популярные фишинговые схемы (несуществующие ссылки, мошенничество с использованием брендов, подложные лотереи).

20. Какие способы защиты от социальной инженерии существуют? Охарактеризуйте основные защитные методы на организационном и техническом уровне.

21 Раскройте концепцию «сетевых войн». Какую роль в них играют наступательные и оборонительные операции в киберпространстве?

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрен учебным планом

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-4.5	Тест, защита лабораторных работ

2	Этапы реализации атак	ПК-4.5	Тест, защита лабораторных работ,
3	Краткое описание некоторых сетевых атак	ПК-4.5	Тест, защита лабораторных работ
4	Технологии обнаружения атак	ПК-4.5	Тест, защита лабораторных работ
5	Социальная инженерия	ПК-4.5	Тест, защита лабораторных работ
6	Проблемы и перспективы применения кибернетического оружия в современной сетцентрической войне	ПК-4.5	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.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131717>

Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/181222>

Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк. — Москва : Высшая школа экономики, 2011. — 572 с. — ISBN 978-5-7598-0698-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/66085>

Дополнительная литература

Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 347 с. — ISBN 978-5-222-26911-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/102279>

Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163844>

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:

Перечень программного обеспечения (open-source)

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/>

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 «Непосредственно и удаленно атакуемые компьютерные системы и сети» читаются лекции, проводятся лабораторные работы.

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.

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 три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]