

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета Гусев П.Ю.

«31» августа 2021 г.



РАБОЧАЯ ПРОГРАММА

дисциплины

«Непосредственно и удаленно атакуемые кибернетические системы
и сети»

Специальность 10.05.02 Информационная безопасность телекоммуникаци-
онных систем

Специализация специализация № 9 "Управление безопасностью телеком-
муникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

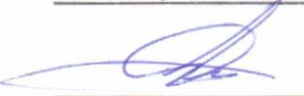
Автор программы

 /А.Е. Дешина/

Заведующий кафедрой Сис-
тем информационной безо-
пасности

 /Остапенко А.Г./

Руководитель ОПОП

 / Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

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

1.2. Задачи освоения дисциплины

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем 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 кибернетические 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 кибернетические системы и сети» направлен на формирование следующих компетенций:

ПК-9.5 - Способен принимать участие в обеспечении функционирования и разработке средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.5	знать особенности обеспечения функционирования и разработки средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)
	уметь анализировать угрозы информационной безопасности в сетях электросвязи

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Непосредственно и удаленно атакуемые кибернетические системы и сети» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	18	18
Самостоятельная работа	108	108
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы	144	144
зач.ед.	4	4

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 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.	4	4	18	26
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	4	4	18	26
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; навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки); SYN-flood, UDP-flood	4	4	18	26
4	Технологии обнаружения атак	методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети	2	2	18	22
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 фи-	2	2	18	22

		шинг. 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	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	2	2	18	22
Итого			18	18	108	144

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-9.5	знать особенности обеспечения функционирования и разработки средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)	знание особенностей обеспечения функционирования и разработки средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать угрозы информационной безопасности в сетях электросвязи	умение анализировать угрозы информационной безопасности в сетях электросвязи	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 7 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-9.5	знать особенности обеспечения функционирования и разработки средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь анализировать угрозы информационной безопасности в сетях электросвязи	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

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

TTI

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

4. Для централизованной аутентификации можно использовать

RADIUS

RETAIL

CONNECT

5. К схемам административных ролей следует отнести

администраторов предприятия

администраторов массива

администраторов блока

6. Из приведенных ниже записей выделите клиентов ISA Server:

Web-прокси

протокол IP

модуль балансировки сети

7. Какие из приведенных ниже записей соответствуют клиентам ISA Server?

DetectIPA

SecureNAT

ModuleDPT

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

ISPData

SecureNAT

NetScan

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

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. 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 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; навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки): SYN-flood, UDP-flood методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети.

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

Концепция «сетевых 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

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	Введение. Классификация атак	ПК-9.5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	Этапы реализации атак	ПК-9.5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Краткое описание некоторых сетевых атак	ПК-9.5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	Технологии обнаружения атак	ПК-9.5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Социальная инженерия	ПК-9.5	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	Проблемы и перспективы применения кибернетического оружия в современной сетцентрической войне	ПК-9.5	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 ме-

тодики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

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>

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>

Дополнительная литература

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>

Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Ин-фра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/148383>

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:

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: <http://www.bdu.fstec.ru>

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: <http://cve.mitre.org>

База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: <https://secuniaresearch.flexerasoftware.com/community/advisories>

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: <https://www.kb.cert.org/vuls>

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: <https://www.exploit-db.com>

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: <https://www.cvedetails.com>

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: <http://www.itsec.ru>

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: <https://www.securitylab.ru/>

Anti-Malware.ru. Электрон. дан. - Режим доступа: <https://www.anti-malware.ru/news>

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: <http://www.iso27000.ru/>

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: <http://securitypolicy.ru/>

SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: <https://searchinform.ru/informatsionnaya-bezopasnost/>

Информационная безопасность предприятия. Электрон. дан. - Режим доступа: [Ekrost.ru](http://ekrost.ru)

<http://att.nica.ru>

<http://www.edu.ru/>

<http://window.edu.ru/window/library>

<http://www.intuit.ru/catalog/>

<http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp>

<https://cchgeu.ru/education/cafedras/kafsib/?docs>

<http://www.eios.vorstu.ru>

<http://e.lanbook.com/> (ЭБС Лань)

<http://IPRbookshop.ru/> (ЭБС IPRbooks)

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 кибернетические 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; 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.
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	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна на-

