

**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 информационные системы  
и сети»

**Специальность** 10.05.03 Информационная безопасность  
автоматизированных систем

**Специализация** специализация N 7 "Анализ безопасности информационных  
систем"

**Квалификация выпускника** специалист по защите информации

**Нормативный период обучения** 5 лет и 6 м.

**Форма обучения** очная

**Год начала подготовки** 2021

**Автор программы**

  
\_\_\_\_\_/Дёшина А.Е./

**Заведующий кафедрой  
Систем информационной  
безопасности**

  
\_\_\_\_\_/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 удаленно атакуемых информационной безопасности в компьютерных систем и сетей, участия в работах по управлению рисками систем защиты информационных 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 сетцентрической войне

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Непосредственно и удаленно атакуемые информационные 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 информационные системы и сети» направлен на формирование следующих компетенций:

ПК-7.5 - Способен обеспечивать безопасность информационных систем, реализующих дистанционный сбор и обработку информации

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.5	знать основные методы и инструменты сбора и систематизации (анализ и оценка) сведений об угрозах НСД в информационных системах
	уметь проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Непосредственно и удаленно атакуемые информационные системы и сети» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий  
**очная форма обучения**

Виды учебной работы	Всего часов	Семестры
		8
<b>Аудиторные занятия (всего)</b>	54	54
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	18	18
<b>Самостоятельная работа</b>	162	162
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы	216	216
зач.ед.	6	6

## 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.	6	4	26	36
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	26	36
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	6	4	26	36
4	Технологии обнаружения атак	методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети	6	2	28	36
5	Социальная инженерия	Популярные фишинговые схемы: несуществующие ссылки; мошенничество с использованием брендов известных корпораций; подложные лотереи; ложные	6	2	28	36

		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	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	28	36
<b>Итого</b>			<b>36</b>	<b>18</b>	<b>162</b>	<b>216</b>

## 5.2 Перечень лабораторных работ

- DDoS основные особенности их организации и защиты. Медленная атака. SlowLoris
  - DDoS основные особенности их организации и защиты. Медленная атака. Slow HTTP POST/GET.
  - DDoS основные особенности их организации и защиты. Медленная атака. Sockstress.
  - DDoS основные особенности их организации и защиты. Атака произвольными пакетами. HTTP-Flood
  - DDoS основные особенности их организации и защиты. Атака произвольными пакетами. SYN-Flood.
  - Атака с помощью SSL
  - Атака почтового сервера. SMTP-Flood
- 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-7.5	знать основные методы и инструменты сбора и систематизации (анализ и оценка) сведений об угрозах НСД в информационных системах	знание основные методы и инструменты сбора и систематизации (анализ и оценка) сведений об угрозах НСД в информационных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	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 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-7.5	знать основные методы и инструменты сбора и систематизации (анализ и оценка) сведений об угрозах НСД в информационных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	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

	автоматизированных систем						
--	---------------------------	--	--	--	--	--	--

## **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**  
**TPI**
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-7.5	Тест, защита лабораторных работ
2	Этапы реализации атак	ПК-7.5	Тест, защита лабораторных работ,
3	Краткое описание некоторых сетевых атак	ПК-7.5	Тест, защита лабораторных работ
4	Технологии обнаружения атак	ПК-7.5	Тест, защита лабораторных работ
5	Социальная инженерия	ПК-7.5	Тест, защита лабораторных работ
6	Проблемы и перспективы применения кибернетического оружия в современной сетцентрической войне	ПК-7.5	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. Озкаяя ; 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 систем 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:

<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/> (ЭБСИРbooks)  
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

## **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 информационные 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: <ul style="list-style-type: none"><li>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;</li><li>- выполнение домашних заданий и расчетов;</li><li>- работа над темами для самостоятельного изучения;</li><li>- участие в работе студенческих научных конференций, олимпиад;</li><li>- подготовка к промежуточной аттестации.</li></ul>
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.