Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«31» 05 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Техника и технология атак злоумышленников в распределенных информационных системах

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*7*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2019

Разработчик рабочей программы:

к.т.н., доцент — (должность, степень, ученое звание)

(подпись)

(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС
(наименование кафедры)

(подпись)

А.Ю. Лошманов
(ФИО)

Заведующий выпускающей кафедрой[1]

(наименование кафедры)

(подпись)

(ФИО)

1 Общие положения

Рабочая программа и фонд оценочных средств дисциплины «Техника и технология атак злоумышленников в распределенных информационных системах» составлены в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Обеспечение информационной безопасности распределенных информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Профессиональная подготовка осуществляется на основе

Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утвержденный Министерства труда и социальной защиты Российской Федерации от от 15 сентября 2016 г. N 522н обобщенные трудовые функции С/02.6 Разработка организационно-распорядительных документов по защите информации в автоматизированных системах Е/02.8 Определение угроз безопасности информации, обрабатываемой автоматизированной системой, В/05.6 Мониторинг защищенности информации в автоматизированных системах

Задачи дисциплины	Сформировать представление о технике и технологии атак злоумышленников на распределенные информационные системы; Сформировать представление о способах защиты от атак злоумышленников распределенные информационные системы.
Основные разделы / темы дисциплины	Основные технологии несанкционированного доступа к сети. Атаки на распределенную информационную систему.

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Техника и технология атак злоумышленников в распределенных информационных системах» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-4 Способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	З1(ПК-4-1) Знать: основные способы несанкционированного доступа к сети	У1(ПК-4-1) Уметь: несанкционированного доступа к сети; уметь осуществлять защиту от несанкционированного доступа к сети	Н1(ПК-4-1) Владеть: навыками реализации несанкционированного доступа к сети

ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	З2(ПК-17- 2) Знать: методы контроля и оценки состояния технической защиты конфиденциальной информации	У2(ПК-17-2) Уметь: разрабатывать необходимые документы по организации технической защиты конфиденциальной информации	Н2(ПК-17-2) Владеть: навыком работы с технической документацией

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Техника и технология атак злоумышленников в распределенных информационных системах» изучается на 4 курсе в 7 семестре.

Дисциплина является базовой дисциплиной, входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: Техническая защита информации.

Знания, умения и навыки, сформированные при изучении дисциплины «Техника и технология атак злоумышленников в распределенных информационных системах», будут востребованы при изучении последующих дисциплин и выполнения выпускной квалификационной работы.

Дисциплина «Техника и технология атак злоумышленников в распределенных информационных системах» в рамках воспитательной работы направлена на развитие творчества, профессиональных умений, ответственности за выполнение учебно-производственных заданий.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	48
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, прак-	32

Объем дисциплины	Всего академических часов
тикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	60
Промежуточная аттестация обучающихся – Зачет с оценкой	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Тема 1 *Понятие сниффинга. Способы реализации.* Знать понятие сниффинга, а так же программы для его осуществления; уметь настраивать фильтры в сниффере; владеть навыками перехвата пакетов, а так же восстанавливать полученную информацию **Тема 2** *Сканирование сети. Обратное сканирование сети. Методы сканирования. Примеры ПО для сканирования.* Знать программы для сканирования сети; уметь понимать данные из программы для сканирования сети; владеть навыками пользования одной из программ для сканирования сети **Тема 3** *Методы и способы несанкционированного подключения к сети.* Знать способы определения сетевых настроек в ЛВС; уметь обнаруживать несанкционированные подключения к сети; владеть навыками несанкционированного подключения к сети *Снифферы*	8		16	30

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Знать понятие сниффинга, а так же программы для его осуществления; уметь настраивать фильтры в сниффере; владеть навыками перехвата пакетов, а так же восстанавливать полученную информацию *Сканирование сети* Знать программы для сканирования сети; уметь понимать данные из программы для сканирования сети; владеть навыками пользования одной из программ для сканирования сети				
Генераторы пакетов. Понятие имперсонализации. Знать понятие имперсонации; уметь распознавать несанкционированные подключения к сети; владеть навыками генерации произвольных сетевых пакетов. Атака Man-in-the-middle Знать основные способы атаки man-in-the-middle; уметь предотвращать атаки man-in-the-middle; владеть навыками реализации атаки man-in-the-middle. IP-спуфинг, ARP-спуфинг. Способы реализации. Знать основные способы атак IP-спуфинг, ARP-спуфинг; уметь предотвращать атаки IP-спуфинг, ARP-спуфинг; владеть навыками реализации атак IP-спуфинг, ARP-спуфинг. DDoS атаки. Способы реализации. Знать основные способы DDOS атаки; уметь предотвращать DDOS атаки; владеть навыками реализации DDOS атаки. Несанкционированное подключение к сети Знать способы определения сетевых настроек в ЛВС; уметь обнаруживать несанкционированные подключения к сети; владеть навыками несанкционированного подключения к сети Реализация ARP-спуфинга Знать основные способы атаки ARP-спуфинг; уметь предотвращать атаки ARP-спуфинг; владеть навыками реализации атаки ARP-	8		16	30

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
спуфинг. Реализация Man-in-the-middle атаки Знать основные способы атаки man-in-the-middle; уметь предотвращать атаки man-in-the-middle; владеть навыками реализации атаки man-in-the-middle. Тема 6 Реализация DDOS атаки. Знать основные способы DDOS атаки; уметь предотвращать DDOS атаки; владеть навыками реализации DDOS атаки.				
ИТОГО по дисциплине	**16**		**32**	**60**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	10
Подготовка к занятиям семинарского типа	10
Подготовка и оформление РГР	40
Всего	60

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Беленькая, М. Н. Администрирование в информационных системах : учебное по-

собие для вузов / М. Н. Беленькая, С. Т. Малиновский, Н. В. Яковенко. - Москва : Горячая линия-Телеком, 2018. - 408 с. - ISBN 978-5-9912-0418-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1195564 (дата обращения: 28.09.2020). – Режим доступа: по подписке.

2. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189333 (дата обращения: 28.09.2020). – Режим доступа: по подписке.

3. Войтов Н. М. Курс RH-133. Администрирование ОС Red Hat Enterprise Linux. Конспект лекций и практические работы ver. 1.10 [Электронный ресурс] / Войтов Н. М. - ДМК Пресс, 2011. Режим доступа: http://www.biblioclub.ru/index.php?page=book&id=129920 3

4. Власов Ю. В. Администрирование сетей на платформе MS Windows Server: учебное пособие [Электронный ресурс] / Власов Ю. В., Рицкова Т. И. - Интернет-Университет Информационных Технологий, 2008. Режим доступа: http://biblioclub.ru/index.php?page=book&id=233291

8.2 Дополнительная литература

1. Трещев И.А., Кожин И.А. Эмуляторы и симуляторы сетей ЭВМ : Для студентов технических специальностей / Издательские решения, 2020. — 166 с. ISBN 978-5-4493-9748-5

2. Трещев И.А., Вильдяйкин Г.Ф., Ватолина А.С. Технология сканирования на наличие уязвимостей / Издательские решения, 2020. — 136 с. ISBN 978-5-4498-9961-3

3. Трещев И.А. Сети и телекоммуникации : Для студентов / Издательские решения, 2020. — 140 с.ISBN 978-5-4493-9742-3

4. Трещев И.А., Григорьев Я.Ю. Проектирование и защита информационных систем / Издательские решения, 2020. — 86 с. ISBN 978-5-4498-9392-5

5. Трещев И.А., Кожин И.А., Вильдяйкин Г.Ф. Безопасность операционных систем : Часть 1. RAID, восстановление файлов, metasploit / Издательские решения, 2020. — 160 с. ISBN 978-5-4498-9599-8 (т. 1) ISBN 978-5-4498-9600-1

6. Трещев И.А., Кожин И. Безопасность вычислительных сетей : Практические аспекты / Издательские решения, 2020. — 126 с. ISBN 978-5-4498-9454-0

7. Трещев И.А. Техника и технология атак злоумышленников в распределенных информационных системах : Для студентов технических специальностей / Издательские решения, 2020. — 102 с. ISBN 978-5-4493-9419-4

8. Трещев И.А., Кожин И.А., Вильдяйкин Г.Ф. Администрирование распределенных информационных систем : Часть 1. Администрирование информационных систем / Издательские решения, 2020. — 170 с. ISBN 978-5-4498-9912-5 (т. 1) ISBN 978-5-4498-9913-2

9. Трещев И.А., Ватолина А.С., Сериков В.А. Техника и технология атак злоумышленников в распределенных информационных системах. Часть 1 Рекогнасцировка, начала атак. / Издательские решения, 2021. — 160 с. ISBN 978-5-0055-1061-7 (т. 1) ISBN 978-5-0055-1062-4

10. Трещев И.А., Прокофьев С.В. Администрирование распределенных информационных систем. Часть 2 технологии информационных систем. / Издательские решения, 2021. — 228 с. ISBN 978-5-0055-0683-2 (т. 2) ISBN 978-5-4498-9913-2

11. Трещев И.А., Прокофьев С.В. Безопасность операционных систем. Часть 2 Операционные системы, уязвимости. / Издательские решения, 2021. — 262 с. ISBN 978-5-0055-0940-6 (т. 2) ISBN 978-5-4498-9600-1

8.2 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Техника и технология атак злоумышленников в распределенных информационных системах» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к лабораторным занятиям, изучение теоретических разделов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Техника и технология атак злоумышленников в распределенных информационных системах» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление контрольной работы.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты контрольной работы;

Контрольная работа и отчеты по лабораторным работам должны быть оформлены в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

8.3 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – **Ошибка! Недопустимый объект гиперссылки.**.
2. Консультант+

8.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.5 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог содержащая необходимые модули для анализа защищенности	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Гипервизор Virtual Box или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое
Виртуальные машины согласно перечню из фондов оценочных средств для дисциплины	Свободно-распространяемое
Parrot OS	Свободно-распространяемое

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные

образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

В данной дисциплине в рамках самостоятельной работы студенты выполняют одну курсовую работу состоящую из двух частей.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению курсовой работы

Теоретическая часть курсовой работы выполняется по установленным темам с использованием практических материалов. К каждой теме курсовой работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или

учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_202_, оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Техника и технология атак злоумышленников в распределенных информационных системах

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*7*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-4 Способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	З1(ПК-4-1) Знать: основные способы несанкционированного доступа к сети	У1(ПК-4-1) Уметь: несанкционированного доступа к сети; уметь осуществлять защиту от несанкционированного доступа к сети	Н1(ПК-4-1) Владеть: навыками реализации несанкционированного доступа к сети
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	З2(ПК-17- 2) Знать: методы контроля и оценки состояния технической защиты конфиденциальной информации	У2(ПК-17-2) Уметь: разрабатывать необходимые документы по организации технической защиты конфиденциальной информации	Н2(ПК-17-2) Владеть: навыком работы с технической документацией

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
РГР	ПК-4, ПК-17	Расчетно-графическая работа	Умение проводить анализ атак на распределенные информационные системы
Тема 1 Снифферы.	ПК-4, ПК-17	Лабораторная работа 1	Владеет теорией по предмету. Задание на лабораторной работы выполняет верно.
Тема 2 Сканирование сети.	ПК-4, ПК-	Лабора-	Владеет теорией по

	17	торная работа 2	предмету. Задание на лабораторной работы выполняет верно.
Тема 3 Несанкционированное подключение к сети.	ПК-4, ПК-17	Лабораторная работа 3	Владеет теорией по предмету. Задание на лабораторной работы выполняет верно.
Тема 4 Реализация ARP-спуфинга.	ПК-4, ПК-17	Лабораторная работа 4	Владеет теорией по предмету. Задание на лабораторной работы выполняет верно.
Тема 5 Реализация Man-in-the-middle атаки.	ПК-4, ПК-17	Лабораторная работа 5	Владеет теорией по предмету. Задание на лабораторной работы выполняет верно.
Тема 6 Реализация DDOS атаки.	ПК-4, ПК-17	Лабораторная работа 6	Владеет теорией по предмету. Задание на лабораторной работы выполняет верно.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 6 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
7 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и уме-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				ния рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Лабораторная работа 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Лабораторная работа 4	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
5	Лабораторная работа 5	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания,

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
6	Лабораторная работа 6	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
7	Расчетно-графическая работа	В течение семестра	15 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите. 10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
Текущий контроль:			75 баллов	
ИТОГО:			75 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень); 85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Лабораторная работа №1

1) Собрать лабораторный стенд согласно рисунку 1.

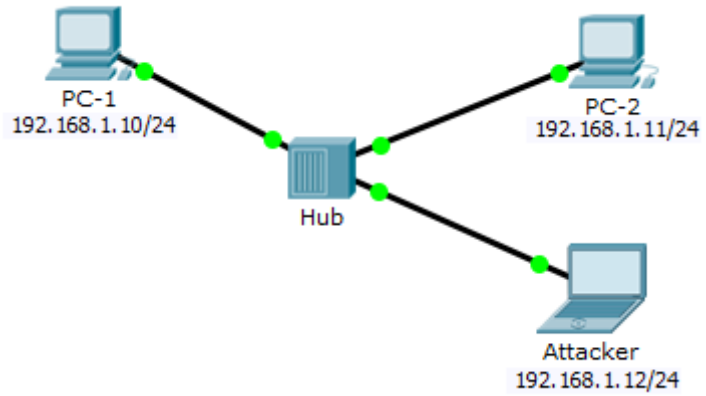

Рисунок 1 – Лабораторный стенд

2) Передавая echo-запрос с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark».

3) Передавая файлы («.txt», «.png», «.rar») по протоколу «SMB» с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark». Восстановить перехваченные файлы.

4) Выполняя авторизацию на FTP-сервере с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark». Авторизоваться с «Attacker» на FTP-сервере.

5) Выполняя авторизацию по протоколу telnet с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark». Авторизоваться с «Attacker» по telnet.

6) Выполнить перехват протокола SMTP используя сниффер «Wireshark». Проанализировать полученные данные.

7) Выполнить перехват протокола POP3 используя сниффер «Wireshark». Проанализировать полученные данные.

8) Выполнить перехват протокола IMAP используя сниффер «Wireshark». Проанализировать полученные данные.

9) Выполнить перехват протокола LDAP используя сниффер «Wireshark». Проанализировать полученные данные.

10) Выполнить перехват протокола SNMP используя сниффер «Wireshark». Проанализировать полученные данные.

11) Выполнить перехват протокола SIP используя сниффер «Wireshark». Проанализировать полученные данные.

12) Выполнить перехват трафика от MS SQL Server используя сниффер «Wireshark». Проанализировать полученные данные.

13) Выполнить перехват трафика от MySQL используя сниффер «Wireshark». Проанализировать полученные данные.

14) Собрать лабораторный стенд согласно рисунку 2.

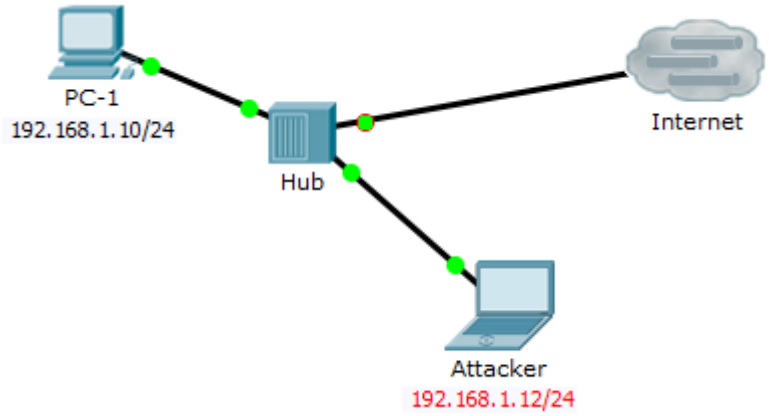

Рисунок 2 – Лабораторный стенд

15) Выполняя авторизацию с «PC-1» на сайте «http://olymp.knastu.ru» по протоколу http, выполнить перехват трафика на «Attacker» используя сниффер «Wireshark». Авторизоваться на сайте «http://olymp.knastu.ru» с «Attacker» по перехваченным данным.

Лабораторная работа №2

Выполнить следующие типы сетевого сканирования:

- ICMP сканирование.
- TCP сканирование.
- Xmas сканирование.
- Null сканирование.
- IDLE сканирование.
- UDP сканирование.
- ACK сканирование.
- Определить операционную систему.
- Сканирование уязвимостей.

Исследовать все типы сканирования при помощи сниффера Wireshark.

Лабораторная работа №3

1) Собрать лабораторный стенд согласно рисунку 3.

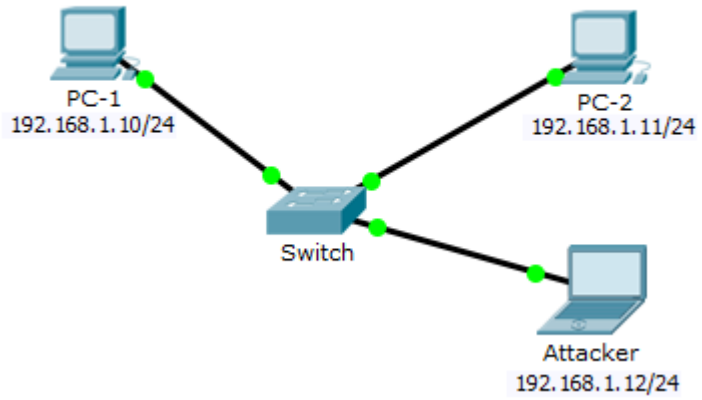

Рисунок 3 – Лабораторный стенд

2) Выполнить атаку MAC-флудинг на «Switch». Передавая echo-запрос с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark».

Лабораторная работа №4

1) Собрать лабораторный стенд согласно рисунку 4.

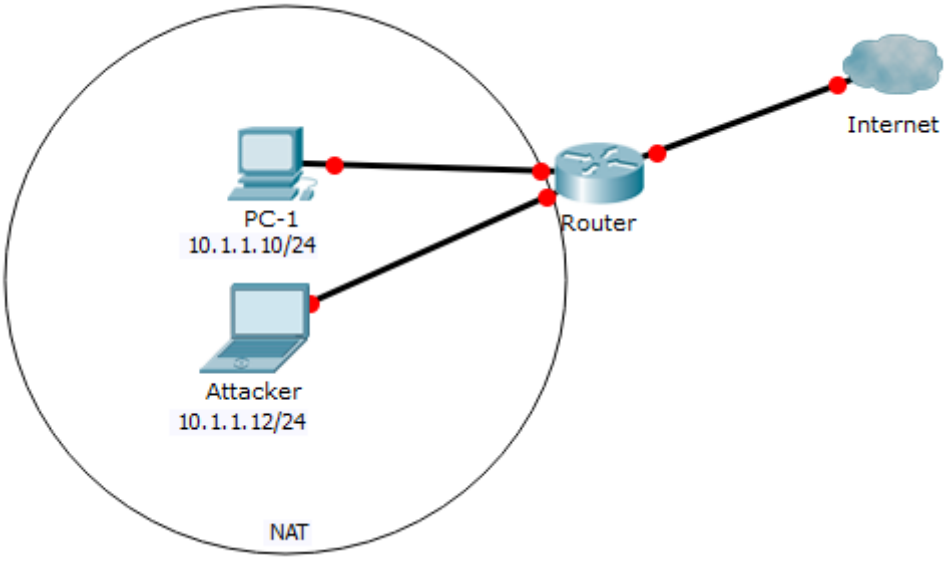

Рисунок 4 – Лабораторный стенд

2) Выполнить атаку ARP-спуфинг на «Router», используя программу «Cain & Abel». Выполняя авторизацию с «PC-1» на сайте «http://olymp.knastu.ru» по протоколу

http, выполнить перехват трафика на «Attacker» используя программу «Cain & Abel». Авторизоваться на сайте «http://olymp.knastu.ru» с «Attacker» по перехваченным данным.

Лабораторная работа №5

1) Собрать лабораторный стенд согласно рисунку 5.

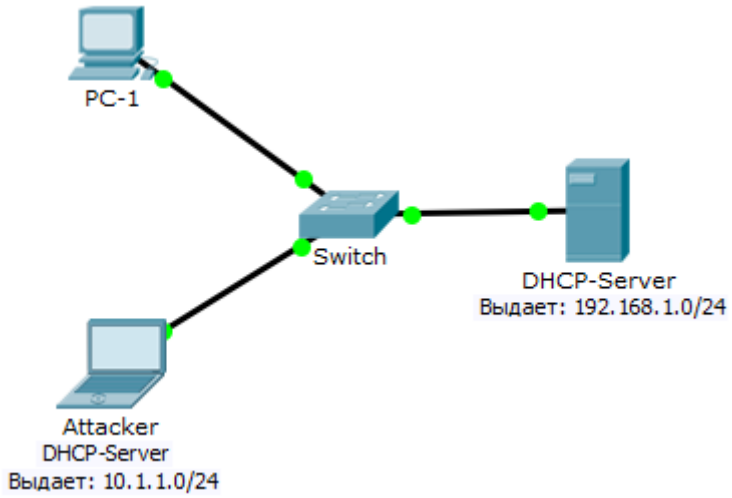

Рисунок 5 – Лабораторный стенд

2) Выполнить атаку DHCP Starvation на «DHCP-Server». Выкачать весь диапазон IP-адресов с «DHCP-Server». После чего развернуть DHCP на «Attacker». Настроить маршрутизацию между двумя сетями на «Attacker».

3) Подключить «PC-2» в «Switch» (рисунок 6).

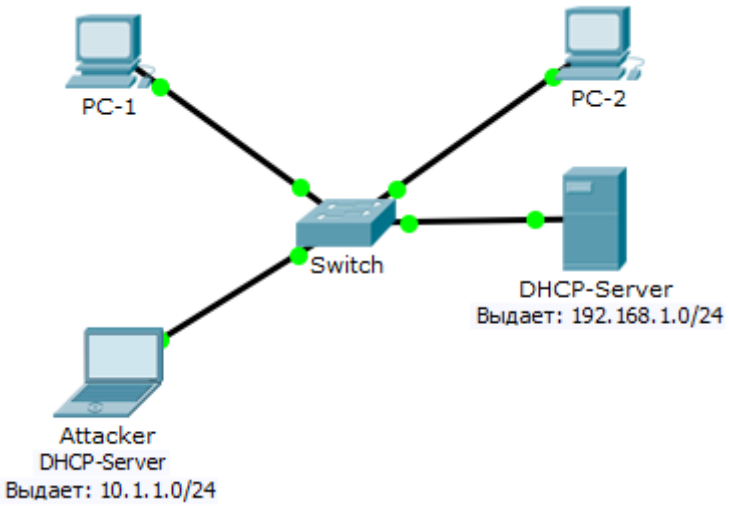

Рисунок 6 – Лабораторный стенд

4) Передавая echo-запрос с «PC-1» на «PC-2», выполнить перехват трафика на «Attacker» используя сниффер «Wireshark».

Лабораторная работа №6

1) Собрать лабораторный стенд согласно рисунку 7.

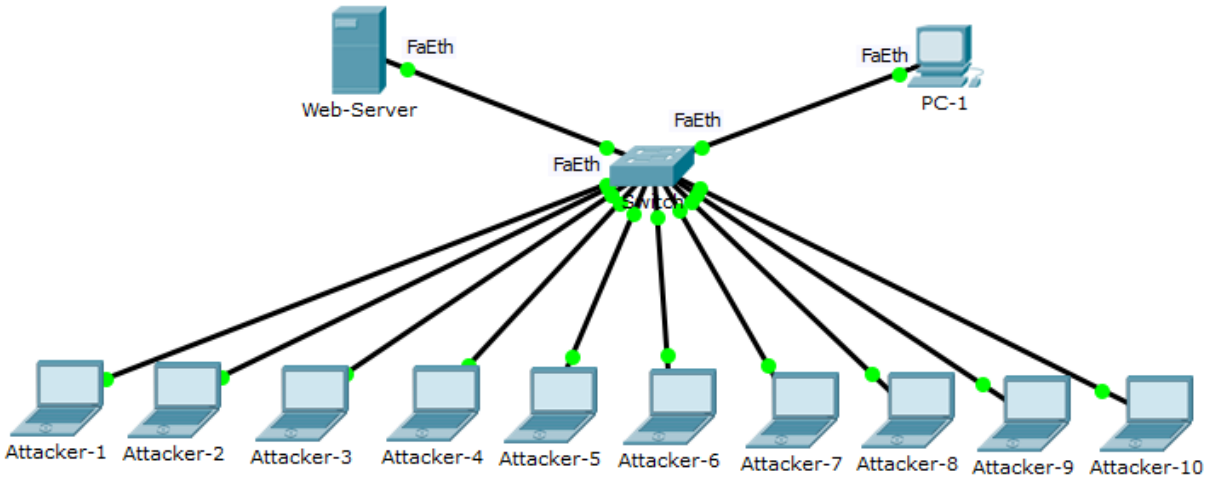

Рисунок 7 – Лабораторный стенд

2) Выполнить атаку DDoS с «Attacker-$\overline{1,10}$» на «Web-Server», используя ICMP-флуд. «PC-1» должен перестать получать услуги «Web-Server».

3) Выполнить атаку DDoS с «Attacker-$\overline{1,10}$» на «Web-Server», используя TCP-флуд. «PC-1» должен перестать получать услуги «Web-Server».

4) Выполнить атаку DDoS с «Attacker-$\overline{1,10}$» на «Web-Server», используя UDP-флуд. «PC-1» должен перестать получать услуги «Web-Server».

5) Выполнить атаку DDoS с «Attacker-$\overline{1,10}$» на «Web-Server», используя HTTP-флуд. «PC-1» должен перестать получать услуги «Web-Server».

6) Выполнить атаку DDoS с «Attacker-$\overline{1,10}$» на «Web-Server», вызвав недостаток ресурсов (ЦП, ОЗУ). «PC-1» должен перестать получать услуги «Web-Server».

Задания для расчетно-графической работы

Разобрать самостоятельно одну из предложенных тем. Описать теоретическую основу темы. Продемонстрировать практическое применение темы.

Темы курсовых работ:

1) Атаки на протокол HTTPS
2) Атаки на сети Wi-Fi
3) SQL-инъекции
4) NoSQL-инъекции
5) XSS-атаки
6) IP-спуфинг
7) DNS-спуфинг
8) Создание туннелей
9) Атака «Состояние гонки»
10) Сканирование сети
11) DHCP истощение
12) MAC-флудинг
13) Атаки MITM
14) DDOS-атаки
15) Атаки на VLAN
16) Уязвимости протоколов аутентификации Windows
17) Уязвимости протоколов аутентификации Linux
18) Уязвимости протоколов аутентификации Web-приложений
19) Уязвимости протоколов передачи данных
20) Уязвимости VoIP
21) Уязвимость STP

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД