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)
«15» 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность сетей ЭВМ

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)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

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

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

доцент, к.т.н. _____ _____ Гришев И.А.
(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ А.Ю. Лоцманов
(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа и фонд оценочных средств дисциплины «Безопасность сетей ЭВМ» 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".

Задачи дисциплины	изучение основных принципов функционирования сетевых протоколов; привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей; изучение основных угроз в сетях ЭВМ и методов противодействия им;
Основные разделы / темы дисциплины	Безопасность сетей ЭВМ, сетевые операционные системы, сканирование

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

Процесс изучения дисциплины «Безопасность сетей ЭВМ» 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			
Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24)	З1(ПК-24-2) Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей	У1(ПК-24-2) Проектировать и администрировать компьютерные сети, реализовывать политику безопасности в сетях ЭВМ	Н1(ПК-24-2) Навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности

Способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27)	З1(ПК-27-3) Последовательность и содержание этапов построения компьютерных сетей	У1(ПК-27-3) Эффективно использовать различные методы и средства защиты информации для компьютерных сетей	Н1(ПК-27-3) Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности
Профессионально-специализированные			
Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3)	З1(ПСК-7.3-1) Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ	У1(ПСК-7.3-1) Проводить мониторинг угроз безопасности компьютерных сетей	Н1(ПК-7.3-1) Навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Безопасность сетей ЭВМ» 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: Безопасность операционных систем, Информационная безопасность объектов критической информационной инфраструктуры, безопасность систем баз данных, внутренний и внешний аудит информационной безопасности.

Знания, умения и навыки, сформированные при изучении дисциплины «Безопасность сетей ЭВМ», будут востребованы при выполнения выпускной квалификационной работы.

Дисциплина «Безопасность сетей ЭВМ»» 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 4 зачетные единицы, 144 академических часа.

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	144
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, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
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 – Экзамен	36

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	
Безопасность сетей ЭВМ. Распределенная обработка данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Системы кли-	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	
ент-сервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети. Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендаций по построению систем защиты. Влияние человеческого фактора на сетевую безопасность. Маршрутизаторы, межсетевые экраны (МЭ). Основные схемы применения МЭ. Абонентское шифрование. Виртуальные частные сети. Защита компонентов сети от НСД. Идентификация и аутентификация абонентов сети. Методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях. Сканирование на наличие уязвимостей				
Сетевые операционные системы, атаки. Сетевые операционные системы (ОС) NetWare, Windows, Unix. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений. Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по	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	
реализации политики безопасности. Поддержание и модификация политики безопасности. Использование брандмауэра в сетевых ОС. Удаленный доступ к сетевым ОС. Демилитаризованная зона. Процесс стандартизации Интернет. Базовые протоколы семейства TCP/IP. Протоколы управления сетью. Прикладные протоколы и службы. Электронный документооборот. Особенности реализации и взаимодействия приложений на различных платформах. Программирование для WWW. Доступ к базам данных в Интернет. Ограничения современной архитектуры Интернет. Новые стандарты и протоколы. Языковые средства представления информации в Интернет. Сети интранет. Основные принципы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет. Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Безопасность Java. Стандарты и протоколы защищенного электронного документооборота. Защита программного окружения рабочей станции. Защита персональных данных. Защита от вирусов. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет. Перехват				

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	
пакетов в ЛВС				
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	5
Подготовка к лабораторным работам	5
Подготовка и оформление РГР	50
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. Компьютерные сети: Учебное пособие / Кузин А.В., Кузин Д.А. - 3-е изд., перераб. и доп. - 2015. - 192 с.: – [ZNANIUM.COM] - Режим доступа: http://znanium.com/catalog/product/536468, ограниченный, Загл. с экрана.

2. Сети связи и системы коммутации: Учебное пособие / Паринов А.В., Ролдугин С.В., Мельник В.А. [ZNANIUM.COM] 2015. - 178 с. - Режим доступа: http://znanium.com/catalog/product/923309, ограниченный, Загл. с экрана.

3. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - 3-е изд., испр. и доп. - М.: Форум, 2008. - 448 с.: ил.; 60x90 1/16. - [ZNANIUM.COM] - Режим доступа: http://znanium.com/catalog/product/163728, ограниченный, Загл. с экрана.

8.2 Дополнительная литература

1. Мэйволд Э. Безопасность сетей [Электронный ресурс]/ Мэйволд Э.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2015.— 571 с.— Режим доступа: http://www.iprbookshop.ru/73727.html // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

2. Зиангирова Л.Ф. Вычислительные системы, сети и телекоммуникации [Электронный ресурс]: учебно-методическое пособие/ Зиангирова Л.Ф.— Электрон. текстовые данные. — 2015.— 150 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/67231.html, ограниченный. – Загл. с экрана.

3 И.А. Трещев, Г.Ф. Вильдяйкин, И.А. Кожин Безопасность операционных систем. Часть 1. Raid, восстановление файлов, metasploit // Издательские решения 2020 - 140с.

4 И.А. Трещев, Г.Ф. Вильдяйкин, И.А. Кожин. Администрирование распределенных информационных систем. Часть 1. Администрирование информационных систем. // Издательские решения 2020 - 162с.

5 И.А. Трещев, С.В. Прокофьев. Администрирование распределенных информационных систем. Часть 2. Технологии информационных систем // Издательские решения 2021 - 228с.

6 И.А. Трещев, С.В. Прокофьев. Безопасность операционных систем. Часть 2. Операционные системы, уязвимости. // Издательские решения 2021 - 262с.

7 И.А. Трещев Анализ защищенности распределенных информационных систем. // Издательские решения 2020 - 102с.

8 В.А. Тихомиров Операционные системы. Ч. 2. Операционные системы защищенного режима работы процессора: Учеб. пособие. – Комсомольск-на-Амуре: ГОУВПО «КнАГТУ», 2003. - 206 с.

9 А.А. Хусаинов, Н.Н. Михайлова Архитектура вычислительных систем: Учеб. пособие / А.А. Хусаинов, Н.Н. Михайлова. – Комсомольск-на-Амуре: Государственное образовательное учреждение высшего профессионального образования «Комсомольский-на-Амуре гос. техн. ун-т», 2007. – 123 с.

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Безопасность сетей ЭВМ» 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 «Безопасность сетей ЭВМ» 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 РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

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

– выполнения и защиты РГР;

Расчетно-графические работы должны быть оформлены в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

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

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+

8.5 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.

8.6 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	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Гипервизор Virtual Box или	Свободно-распространяемое

аналог	
Обозреватель Google Chrome или аналог	Свободно-распространяемое
Cisco Packet Tracer	Распространяется свободно при бесплатной регистрации в сетевой академии Cisco

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 расчетно-графическую 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 расчетно-графической работы

Теоретическая часть расчетно-графической работы выполняется по установленным темам с использованием практических материалов. К каждой теме расчетно-графической 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 безопасности сетей ЭВМ	VipNet Personal FireWall, АРМ с установленной Secret Net Studio 8 системы обнаружения компьютерных атак Выделенные АРМ с установленной Secret Net Studio 8 СОВ 2 шт. АРМ с установленным Snort, АРМ с установленным WireShark, Анализа сетевого траффика Астра межсетевые экраны: CheckPoint Connectra, Cisco ASA 5505, ЦУС Континент, Secret Net Studio 8, 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

Безопасность сетей ЭВМ

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)*	*2020*
Форма обучения	*очная*
Технология обучения	*традиционная*

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

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*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			
Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24)	З1(ПК-24-2) Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей	У1(ПК-24-2) Проектировать и администрировать компьютерные сети, реализовывать политику безопасности в сетях ЭВМ	Н1(ПК-24-2) Навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
Способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27)	З1(ПК-27-3) Последовательность и содержание этапов построения компьютерных сетей	У1(ПК-27-3) Эффективно использовать различные методы и средства защиты информации для компьютерных сетей	Н1(ПК-27-3) Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности
Профессионально-специализированные			

Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3)	З1(ПСК-7.3-1) Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ	У1(ПСК-7.3-1) Проводить мониторинг угроз безопасности компьютерных сетей	Н1(ПК-7.3-1) Навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Показатели оценки**
1. Безопасность сетей ЭВМ	ПСК-7.3 ПК-24	Лабораторная работа № 1 Расчетно-графическая работа №1	Знать основы построения системы защиты ЛВС предприятия
2. Сетевые операционные системы, атаки	ПК-27	Лабораторная работа № 2 Расчетно-графическая работа №1	Знать особенности операционных систем при обеспечении информационной безопасности при функционировании в сети, виды атак
Темы 1,2	ПК-24, ПК-27, ПСК-7.3	Экзамен	Эффективно применять на практике полученные в течении семестра знания и опыт

Промежуточная аттестация в пятом семестре проводится в форме экзамена.

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 3 – Технологическая карта

Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
7 семестр ***Промежуточная аттестация в форме экзамена***			
Лабораторная работа №1	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 4 балла - студент выполнил задание, с

Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
			небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Лабораторная работа работа №2	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 4 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Расчетно-графическая работа № 1	В течение семестра	25 баллов	25 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 20 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 15 баллов - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 10 баллов - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Задача – оценивание уровня усвоенных знаний		20 баллов	20 баллов - студент правильно ответил на теоретический вопрос билета. Показал отличные знания в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы. 15 баллов - студент ответил на теоретический вопрос билета с небольшими неточностями. Показал хорошие знания в рамках усво-

Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
			енного учебного материала. Ответил на большинство дополнительных вопросов. 10 баллов - студент ответил на теоретический вопрос билета с существенными неточностями. Показал удовлетворительные знания в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при ответе на теоретический вопрос билета студент продемонстрировал недостаточный уровень знаний. При ответах на дополнительные вопросы было допущено множество неправильных ответов.
Задача – оценивание уровня усвоенных умений и навыков		15 баллов	15 баллов - студент правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Ответил на все дополнительные вопросы. 10 баллов - студент выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Ответил на большинство дополнительных вопросов. 5 баллов - студент выполнил практическое задание билета с существенными неточностями. Показал удовлетворительные умения в рамках освоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при выполнении практического задания билета студент продемонстрировал недостаточный уровень умений. При ответах на дополнительные вопросы было допущено множество неправильных ответов.
Экзамен		35 баллов	
ИТОГО:		**70 баллов**	

Критерии оценки результатов обучения по дисциплине, включая экзамен:

0 – 64 % от максимально возможной суммы баллов – ***0 – 44 баллов*** - «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);

65 – 74 % от максимально возможной суммы баллов – ***45 – 53 баллов*** - «удовлетворительно» (пороговый (минимальный) уровень);

75 – 84 % от максимально возможной суммы баллов – ***54- 61 балла*** - «хорошо» (средний уровень);

85 – 100 % от максимально возможной суммы баллов – ***60 – 70 баллов*** - «отлично» (высокий (максимальный) уровень).

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характери-

зующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Лабораторная работа №1

Учебные цели: изучить программное обеспечение СканерВС, провести анализ защищённости с использованием сканера уязвимостей СканерВС,

Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

После выполнения лабораторной работы уметь проводить оценку защищённости АРМ, владеть навыками анализа и поиска уязвимостей с использованием сканера уязвимостей СканерВС, построения отчетов по результатам сканирования

Перечень материально-технического обеспечения

Лабораторное оборудование и программное обеспечение: 10 компьютеров на базе Intel Core i5, 1 коммутатор D-link DES-3200-18, сертифицированное и лицензионное программное обеспечение СканерВС.

Студенты проводят полное сканирование отдельно произвольного АРМ из тех что расположены в ЛВС лаборатории возможно свой ноутбук (при условии наличия необходимых средств защиты из пункта 6.8), и отдельно коммутатор.

Краткие теоретические сведения основные сведения по работе со сканером уязвимостей изложены в документе «Руководство пользователя СканерВС».

Порядок выполнения лабораторной работы:

Установить СканерВС (версия на CD и на аппаратном носителе).

Активировать лицензию.

Обновить систему до последней версии.

Создать задачу сканирования.

Настроить профиль сканирования на полное сканирование.

Зарегистрировать узлы сканирования.

Добавить узлов в задачу.

Запустить сканирование для АРМ с отключенными механизмами защиты (антивирус, МЭ, СОВ, брэндмауэр, НСД на базе SNS).

Проанализировать полученные результаты.

Сгенерировать отчет.

Добавить сгенерированный отчета в отчет по лабораторной работе

Выполнить шаги 8-11 для АРМ с включенными механизмами защиты.

Выполнить шаги 8-11 для коммутатора или другого сетевого оборудования.

Контрольные вопросы:

Какие профили сканирования можно использовать, задачи, проекты

Как добавлять IP-адреса в лицензию, обновление дистрибутива

Типы отчетов и их различие, типы сканирования

Особенности лицензии СканерВС

Какие компоненты входят в состав СканерВС

Лабораторная работа №2

Установить WireShark на виртуальную машину VMWare.

Провести исследование приема пакетов APR и ICMTP для этого смоделировать ping между реальной и виртуальной машиной.

Провести исследование приема пакетов сервера DNS сервера.

Освоить применения фильтров Capture.

Освоить применения фильтров Display Filters.

Освоить перехват файлов, картинок при передаче по сети.

Освоить перехват аудиофайлов с прослушиванием аудиодорожки.

Установить на арм систему snort. Продемонстрировать атаку icmp flood и ее фиксацию системой.

Установить Alien Vault и с ее помощью отследить произвольную атаку в сети.

Установить LIOC и HOIC и продемонстрировать DOS или DDOS атаку на хост.

Расчетно-графическая работа №1

Задания 1. Восстановление пароля к оборудованию Cisco

Исходные данные:

1. Список оборудования

- Catalyst 2950 (C2950-1) порт 2001;
- Catalyst 2950 (C2950-2) порт 2002;
- Catalyst 2960 (C2960-1) порт 2003;
- Catalyst 2960 (C2960-2) порт 2004;
- Catalyst 3524 (C3524) порт 2005;
- Router 1841 (R1841) порт 2006;
- Router 2811 (R2811) порт 2007;
- Аппаратный брандмауэр Cisco ASA 5505 (ASA5505) порт 2008;
- консольный сервер, ip-адрес 10.10.1.1
- Wi-Fi-маршрутизатор с DHCP.

2. Лабораторная работа выполняется только на аудиторных занятиях.
3. SSID Cisco LAB, пароль на подключение к Wi-Fi - CiscoP@ssw0rd
4. В связи с особенностями консольного соединения к оборудованию может подключаться только 1 сеанс. Например, если в данный момент времени с Router 1841 кто-то работает, второй подключиться не сможет.
5. При подключении к какому-либо консольному порту логин/пароль - 123/123.
6. Перезагрузка коммутаторов и ASA5505 выполняется вручную, при выключении вилки из розетки.
7. Перезагрузка маршрутизаторов выполняется при нажатии кнопки ВЫКЛ на устройстве.

Ход работы:

1. Для выполнения работы необходимо выполнить процедуру password recovery на сетевом оборудовании:

- Catalyst 2950, Catalyst 2960, Catalyst 3524, Router 1841; Router 2811; Cisco ASA 5505.

2. Подключение к оборудованию: **telnet *ip-адрес порт***. Например, для подключения к Router 2811 нужно выполнить в командной строке: **telnet 10.10.1.1 2007**.
3. Выполнение процедуры password recovery многовариантно, т.е. единого алгоритма нет, у каждого он может быть своим. Пошаговые инструкции лежат в папке Password Recovery.
4. Процедура password recovery считается выполненной после того, как студент смог войти в привилегированный режим работы устройства, показав это преподавателю.
5. Коммутаторы настроены с enable password и отключенной авторизацией консольного порта. Для процедуры password recovery достаточно изменить пароль на enable password.

6. Маршрутизаторы настроены с enable password, enable secret и line con 0. Для процедуры password recovery достаточно изменить пароль на enable secret и line con 0.

7. Cisco ASA 5505 настроена с enable password и отключенной авторизацией консольного порта. Для процедуры password recovery достаточно изменить пароль на enable password.

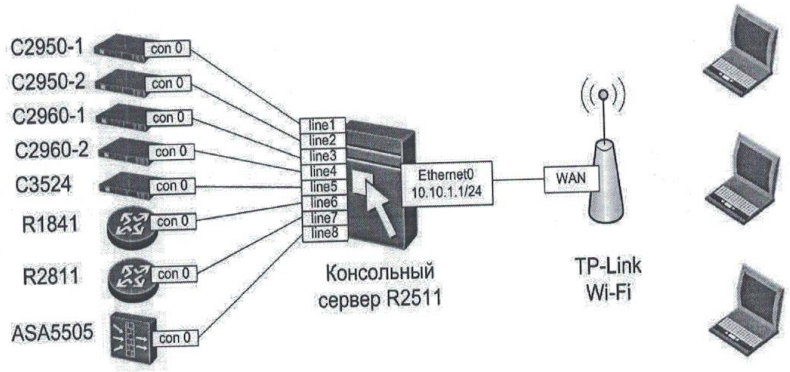


Рисунок схема стенда для выполнения задания

Задание 2

Базовая настройка ASA 5505

Исходные данные:

1. № – номер вашего варианта.
2. X – число, которое нужно выбрать по определенным правилам из некоторого множества.
3. DR – маршрут по умолчанию.
4. На всех маршрутизаторах логин/пароль cisco.
5. На ASA 5505 enable password пустой.
6. На схемах красным цветом помечаются области, где необходимо выполнить настройку.
7. В конфигурации красным цветом помечаются места, которые необходимо изменить.
8. В конфигурации зеленым цветом помечаются имена объектов и переменных.
9. В рамках Lab2-1 базовая настройка R, R1 и ISP уже выполнена. Донастройка требуется только в тех частях схемы дизайна сети, которые помечены красным цветом.
10. При проверке ping и попытке открыть сайт cisco.com пакеты могут начать ходить не сразу, а только с второй-третьей попытки.
11. После выполнения каждой задачи, на всем оборудовании, где выполнялась настройка, необходимо сохранять конфигурацию с помощью команды copy run start, либо ее краткого аналога write (для Cisco ASA – write memory).
12. Объекты изучения ASA 5505:

- настройка интерфейсов и VLAN;
- настройка DHCP;
- настройка Objects и object-groups;
- настройка правил NAT;
- настройка class-map;

- настройка policy-map;
- настройка service-policy.

Задачи:

1. Настройка статической маршрутизации на R, R1 и ISP.
2. Настройка LAN за R1.
3. Настройка соединения R с ASA5505.
4. Настройка ASA5505 и LAN за ASA5505.

Ход работы:

1. На R и R1 выполняется настройка маршрута по умолчанию в сторону ISP.

ip route 0.0.0.0 0.0.0.0 10.5.5.13 1
ip route 0.0.0.0 0.0.0.0 10.16.1.5 1

Проверка: ping с R и R1 на ip-адрес 8.8.8.8 должен проходить.

На ISP настраиваются маршруты к сетям 192.168.1№.0/29 и 192.168.№.128/26.

ip route 192.168.111.0 255.255.255.248 10.5.5.14
ip route 192.168.11.128 255.255.255.192 10.16.1.6

Проверка настройки статической маршрутизации выполняется в следующей задаче.

2. На R1 настраивается LAN-интерфейс.

description LAN
no shutdown
ip address 192.168.11.62 255.255.255.192

После того, как интерфейс «апнулся», выполняется настройка сетевой карты PC1.

ip-address	192.168.11.1
mask	255.255.255.192
default gateway	192.168.11.62
dns	8.8.8.8

Проверка: ping с R на ip-адрес PC1 должен проходить, ping с PC1 на 8.8.8.8 должен проходить, сайт cisco.com должен открываться.

3. На R настраивается LAN-интерфейс.

description LAN_ASA5505
no shutdown
ip address 192.168.111.6 255.255.255.248

Проверка: ping с PC1 на ip-адрес LAN-интерфейса R должен проходить.

4. Переименование Cisco ASA.

hostname ASA5505

Выполняется настройка интерфейсов. WAN-порт – Ethernet0/0, LAN-порт – Ethernet0/1. Vlan 3 добавляется на WAN-порт, vlan 2 на LAN-порт.

interface Ethernet0/0
switchport access vlan 3
interface Ethernet0/1
switchport access vlan 2

Настройка и именование vlan-интерфейсов.

Команда nameif не просто дает описание интерфейса, но и дает этому интерфейсу имя в системе. После того, как vlan-интерфейсу дано имя, при дальнейшей конфигурации появляется возможность указывать не системное имя (vlan 2), а его nameif (inside).

interface vlan 2
nameif inside

После появится системное сообщение, что уровень безопасности для данного vlan выбран по умолчанию как 100 (т.е. самый высокий уровень безопасности). Трафик из этой

сети инспектируется, и создаются автоматические правила, разрешающие прохождение трафика из LAN в WAN.

INFO: Security level for "inside" set to 100 by default.

Параметр 100 рекомендуется устанавливать на порты, роль которых inside, т.е. на те порты, которые подключены к LAN.

Настройка ip-адреса vlan 2.

ip address 192.168.11.62 255.255.255.192

Аналогично выполняется настройка vlan 3.

interface vlan 3
nameif outside

После появится системное сообщение о том, что уровень безопасности для данного vlan выбран по умолчанию как 0 (т.е. самый низкий уровень безопасности).

INFO: Security level for "outside" set to 0 by default.

Параметр security-level 0 говорит о том, что для трафика из LAN будут создаваться автоматические правила при инициации сеанса из LAN в WAN. А при попытке инициации сеанса связи из WAN в LAN трафик будет отброшен.

Настройка ip-адреса vlan 3.

ip address 192.168.111.5 255.255.255.248

Настройка маршрута по умолчанию во внешнюю сеть.

route outside 0.0.0.0 0.0.0.0 192.168.111.6 1 // to router R

Настройка объекта для всех сетей.

object network OBJ_GENERIC_ALL11
subnet 0.0.0.0 0.0.0.0

Настройка правил NAT для трансляции inside-адресов в outside-адрес.

object network OBJ_GENERIC_ALL11
nat (inside,outside) dynamic interface

Настройка class-map.

class-map inspection_default11
match default-inspection-traffic

Настройка policy-map для фильтрации пакетов DNS-запросов, размер которых превышает 512 байт.

policy-map type inspect dns preset_dns_map11
parameters
message-length maximum 512

Настройка глобальной политики global_policy для анализа трафика и фильтрации некоторых протоколов прикладного уровня.

policy-map global_policy
class inspection_default11
inspect dns preset_dns_map11
inspect ftp
inspect h323
inspect http
inspect icmp
inspect tftp

Включение политики global_policy

service-policy global_policy global

Проверка: ping с ASA5505 на 8.8.8.8 должен проходить.

Настройка DHCP.

Адресное пространство рекомендуется выделить на 15-30 ip-адресов. В рамках симулятора CPT протокол DHCP на ASA5505 может работать некорректно, а в некоторых случаях CPT может аварийно закрыться с потерей всех данных. Поэтому перед настройкой DHCP на ASA5505 (так же, как и на остальных устройствах) сохраняется конфигурация (write memory), затем сохраняется весь проект CPT, только потом можно приступать к настройке DHCP. Для 100% сохранения выполненной работы рекомендуется скопировать сохраненный проект CPT и открыть его копию для настройки DHCP.

dhcpd address 192.168.11.1-192.168.11.30 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd enable inside

Чтобы проверить корректность настройки DHCP, нужно выполнить команду show run на ASA5505 и посмотреть в конце вывода конфигурации строчки с настройкой DHCP. Если все применилось верно, то должны быть 4 строки, которые начинаются с dhcpd – 3 строки те, что вводились при настройке DHCP, и еще 1 строка dhcpd auto_config outside. После этого ни в коем случае нельзя перезагружать ASA5505, т.к. CPT с вероятностью 99% аварийно завершится. Если dhcpd auto_config outside нет в конфигурации, а по DHCP ASA сообщает PC все ip-параметры, кроме основного шлюза, то на PC все ip-параметры нужно настроить вручную.

Настройка LAN за ASA5505.

Если с DHCP на ASA проблем нет, PC настраивается на автоматический прием настроек, на Server вручную назначается любой свободный ip-адрес из LAN ASA5505 (ip-адрес сервера не должен пересекаться с пулом DHCP), маска подсети, основной шлюз и DNS.

Проверка: ping с PC и Server на 8.8.8.8 должен проходить, сайт cisco.com должен открываться.

Сохранение конфигурации на всех сетевых устройствах, сохранение проекта CPT.

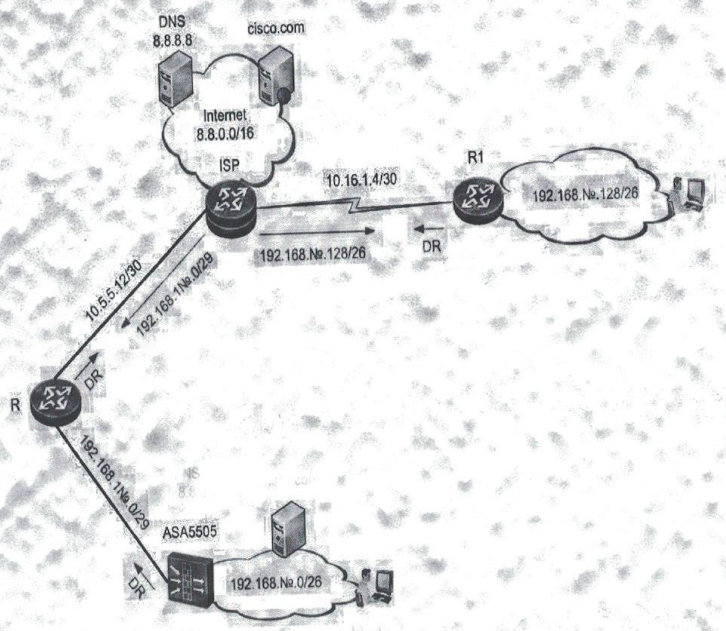


Рисунок схема для настройки

Задание 3 Настройка демилитаризованной зоны на ASA 5505

Исходные данные:

1. № – номер вашего варианта.
2. X – число, которое нужно выбрать по определенным правилам из некоторого множества.
3. DR – маршрут по умолчанию.
4. На всех маршрутизаторах логин/пароль cisco.
5. На ASA 5505 enable password пустой.
6. На схемах красным цветом помечаются области, где необходимо выполнить настройку.
7. В конфигурации красным цветом помечаются места, которые необходимо изменить.
8. В конфигурации зеленым цветом помечаются имена объектов и переменных.
9. При проверке ping и попытке открыть сайты cisco.com и dmz.net пакеты могут начать ходить не сразу, а только с второй-третьей попытки.
10. После выполнения каждой задачи, на всем оборудовании, где выполнялась настройка, необходимо сохранять конфигурацию с помощью команды copy run start, либо ее краткого аналога write (для Cisco ASA – write memory).
11. Объекты изучения ASA 5505:

- настройка интерфейсов и VLAN;
- настройка DHCP;
- настройка Objects и object-groups;
- настройка NAT/PAT;
- настройка class-map;

- настройка policy-map;
- настройка service-policy;
- настройка DMZ;
- настройка SNAT;
- настройка extended ACL.

Задачи:

Настройка соединения ASA5505 и ISP.

Базовая настройка ASA5505 и LAN за ASA5505.

Настройка DMZ.

Настройка SNAT и ACL.

Ход работы:

На ISP настраивается интерфейс в сторону ASA5505.

```
interface Gig0/1
description ASA5505
no shutdown
ip address 209.1.48.13   255.255.255.248
```

Базовая настройка ASA5505.

```
conf t
hostname ASA5505
interface Ethernet0/0
 switchport access vlan 3
 exit
interface Ethernet0/1
 switchport access vlan 2
 exit
interface vlan 2
 nameif inside
 ip address  192.168.11.62   255.255.255.192
 exit
interface vlan 3
 nameif outside
 ip address  209.1.48.9   255.255.255.248
 exit
route outside   0.0.0.0   0.0.0.0   209.1.48.14  1
class-map inspection_default11
 match default-inspection-traffic
 exit
policy-map global_policy
 class inspection_default11
  inspect dns
  inspect ftp
  inspect h323
  inspect http
  inspect icmp
  inspect tftp
  exit
service-policy   global_policy   global
```

exit

write memory

Проверка: ping с ASA5505 на ISP и 8.8.8.8 должен проходить.

Настройка PC в LAN ASA5505.

На PC вручную выполняются ip-настройки (ip-адрес, маска подсети, основной шлюз и DNS-сервер), ip-адрес выбирается любой свободный.

Проверка: ping от PC до ASA5505 должен проходить.

Настройка NAT для inside-subnet (LAN ASA5505).

object network inside-subnet

subnet 192.168.11.0 255.255.255.192

nat (inside,outside) dynamic interface

Проверка: ping от PC до 8.8.8.8 должен проходить, сайт cisco.com должен открываться.

DMZ-server является как веб-сервером, так и сервером DNS для пользователей в DMZ-зоне. Public User`s через браузер открывают сайт dmz.net. Public User`s получают ip-настройки по DHCP от ASA5505. Public Hotspot уже настроена и делает трансляцию Wi-Fi в проводной Ethernet, т.е. является транслирующим мостом и работает на L2. Кроме того, на сайт dmz.net должны заходить пользователи из внешней глобальной сети, поэтому на ASA5505 нужно настроить 2 вида NAT для DMZ – NAT с перегрузкой (для того, чтобы Public Users`s могли выходить во внешнюю сеть) и статический (для того, чтобы на веб-страницу DMZ-server`a мог зайти пользователь с PC-External). На ASA5505 нужно включить ACL, а в DNS сервер 8.8.8.8 внести A-запись dmz.net.

Настройка на ASA5505 интерфейсов и VLAN для DMZ.

Для DMZ выбран порт Ethernet0/2 и VLAN 4.

interface Ethernet0/2

switchport access vlan 4

Настройка vlan-интерфейса.

Команда no forward interface Vlan2 запрещает пересылку трафика из DMZ в LAN, т.е. пользователи из DMZ не смогут связаться с PC.

interface vlan 4

no forward interface Vlan2

nameif dmz

security-level 50

ip address 192.168.211.254 255.255.255.0

Проверка: команда show switch vlan показывает имена и статус всех vlan на ASA.

Настройка DHCP на ASA5505 для автоматической выдачи ip-настроек Public User1 и Public User2.

dhcpd address 192.168.211.11-192.168.211.19 dmz

dhcpd dns 192.168.211.1 interface dmz

dhcpd enable dmz

ASA5505 через DHCP сообщает Public User`s, чтобы они свои dns-запросы на разрешение dmz.net в ip-адрес отправляли DNS-службе DMZ-сервера. DMZ-server будет сообщать Public User`s, что ip-адрес dmz.net будет его же собственный адрес – 192.168.2№.1.

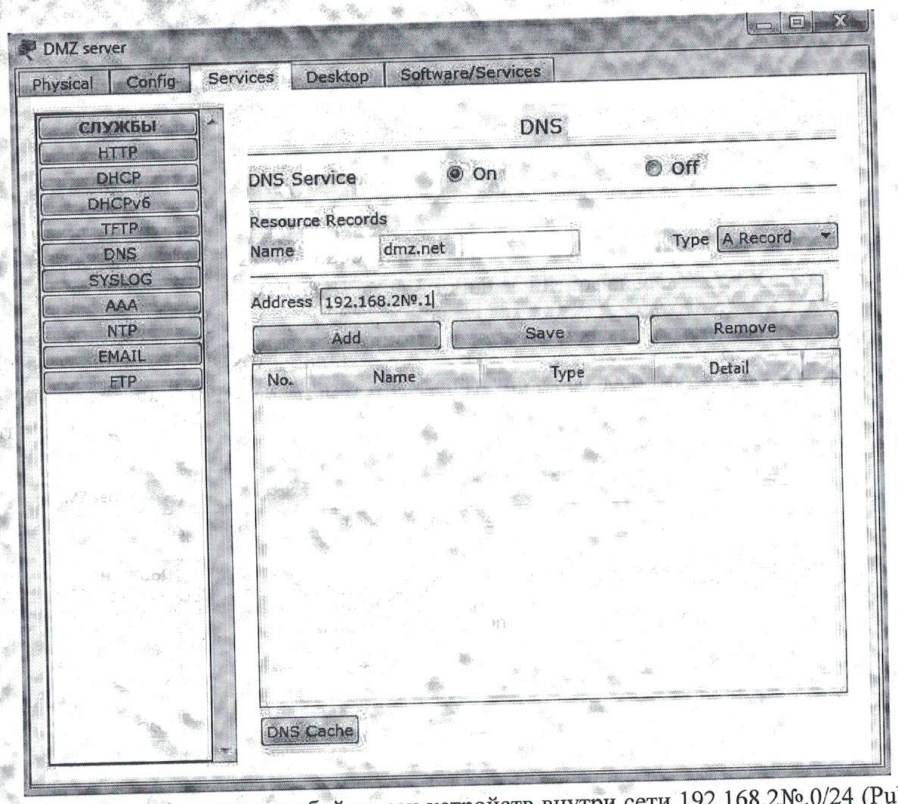
Настройка IP на DMZ-server.

ip-address 192.168.211.1

mask 255.255.255.0
default gateway 192.168.211.254 (ip-адрес интерфейса ASA5505 в этой сети)
dns 192.168.211.1

Настройка DNS на DMZ-server.

Включить службу DNS, указать имя сайта dmz.net и соответствие ему ip-адреса, нажать кнопку add.



Проверка: ping между собой у всех устройств внутри сети 192.168.2№.0/24 (Public Users`s, DMZ-server, ASA5505) должен проходить, у Public User`s должен открываться сайт dmz.net.

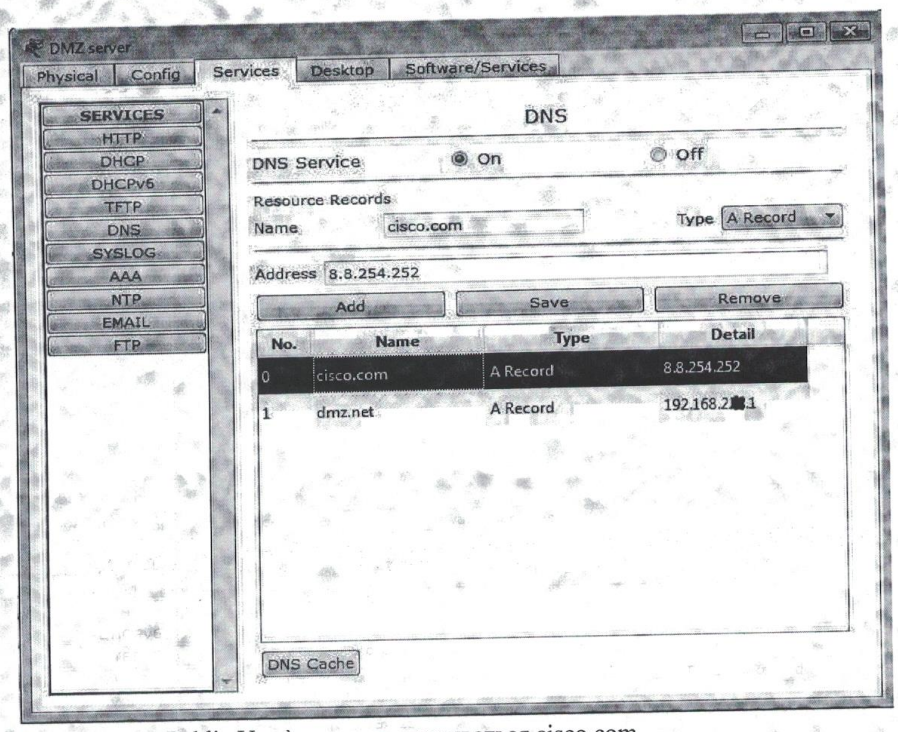
Настройка NAT/PAT для Public Users`s на ASA5505.

Создается object-network и настраивается NAT/PAT.

object network dmz-subnet
subnet 192.168.211.0 255.255.255.0
nat (dmz,outside) dynamic interface

Ping на 8.8.8.8 и 8.8.254.252 должен ходить, но cisco.com не открывается.

Чтобы у Public User`s заработал cisco.com, в DNS-службе DMZ-сервера нужно прописать сопоставление cisco.com ip-адресу 8.8.254.252.



Проверка: у Public User`s должен открываться cisco.com.

5. Настройка SNAT.

Создается объект Webserver-Ext, т.е. переменная для представления DMZ-сервера в сети Интернет. Адрес для переменной выбирается из сети 209.1.48.8/29 и не должен совпадать с назначенными адресами на ASA5505 и ISP.

object network Webserver-Ext
host 209.1.48.12

Теперь нужно создать переменную для представления DMZ-сервера в DMZ LAN и настроить SNAT.

object network Webserver
host 192.168.211.1
nat (dmz,outside) static 209.1.48.12

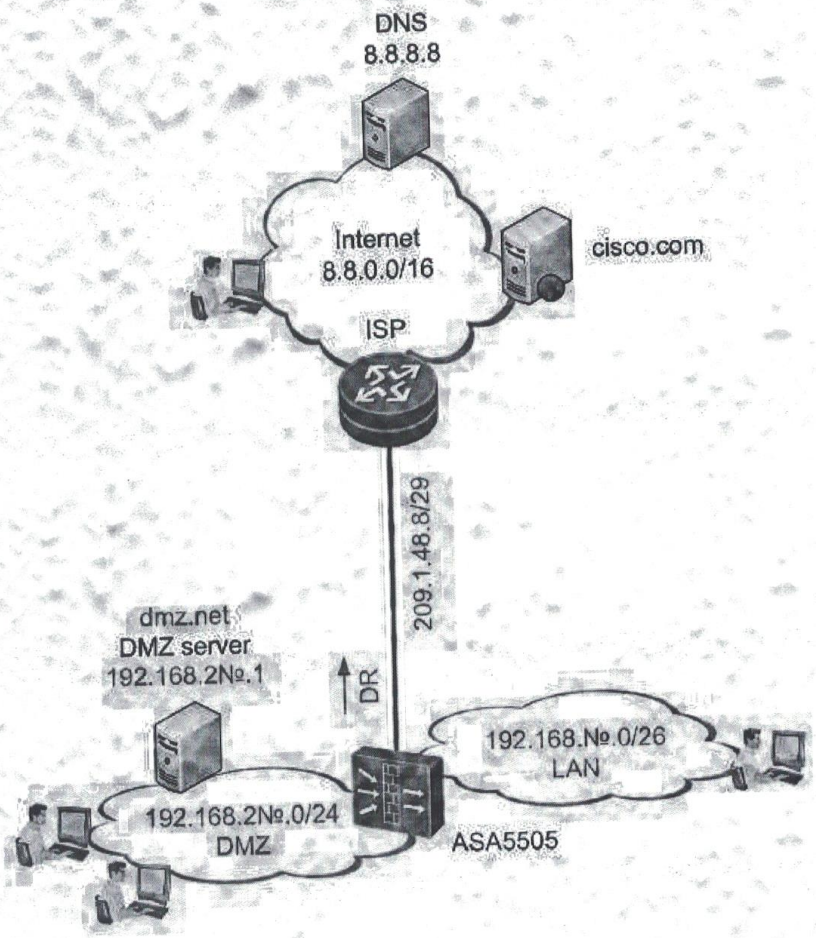
Для обмена http-трафиком между PC-External и DMZ-сервером нужно настроить расширенный список доступа и применить его на внешний интерфейс ASA5505.

access-list Outside extended permit tcp any host 209.1.48.12 eq www
access-group Outside in interface outside

Чтобы dmz.net на PC-External открывался по имени, на DNS-сервере 8.8.8.8 нужно прописать соответствие dmz.net внешнему ip-адресу. В противном случае, чтобы сайт открылся в строке браузера, нужно указать только внешний ip-адрес.

Проверка: На PC-External сайт dmz.net должен открываться.

Сохранение конфигурации на всех сетевых устройствах, сохранение проекта CPT.



Задание 4 Построение клиентских VPN-сетей

Исходные данные:

1. № – номер вашего варианта.
2. X – число, которое нужно выбрать по определенным правилам из некоторого множества.
3. DR – маршрут по умолчанию.
4. На всех маршрутизаторах логин/пароль cisco.
5. На ASA5505 enable password пустой.
6. На схемах красным цветом помечаются области, где необходимо выполнить настройку.
7. В конфигурации красным цветом помечаются места, которые необходимо изменить.
8. В рамках Lab 2-3 базовая настройка R1, R2 и ISP уже выполнена.
9. При проверке ping и попытке открыть сайт cisco.com или Intranet-сервера пакеты могут начать ходить не сразу, а только с второй-третьей попытки.

10. После выполнения каждой задачи, на всем оборудовании, где выполнялась настройка, необходимо сохранять конфигурация с помощью команды copy run start, либо ее краткого аналога write (для Cisco ASA5505 – write memory).

11. Объекты изучения ASA5505:

- ASA Basic;
- настройка DHCP;
- настройка group-policy;
- настройка username и password;
- настройка webvpn.

Задачи:

1. Настройка динамической маршрутизации на R1, R2 и ISP.
2. Настройка LAN R2.
3. Настройка соединения R1 с ASA.
4. Настройка ASA и LAN ASA.
5. Настройка VPN ASA.

Ход работы:

6. На R1, R2 и ISP выполняется настройка OSPF. Ниже приводится типовая конфигурация для настройки динамической маршрутизации.

```
router ospf №
 log-adjacency-changes detail
 network 10.0.0.0   0.255.255.255 area 0
```

На ISP настраивается маршрут по умолчанию в сторону 8.8.0.0/16 и его распределение через OSPF.

```
ip route 0.0.0.0   0.0.0.0   gi0/0   1
router ospf №
 default-information originate
```

Проверка: в выводе команды show ip route на R1 и R2 должен присутствовать маршрут по умолчанию от ISP, а также маршруты к другим сетям, полученные через OSPF. Ping от R1 и R2 до 8.8.8.8 должен проходить.

7. На R2 настраивается интерфейс в сторону LAN (согласно дизайна) и DHCP-сервер. PC2-Client должен получать автоматические настройки по DHCP.

```
description LAN
no shutdown
ip address 10.2№.№.X   /26
```

Настройка DHCP на R2.

```
ip dhcp pool LAN
 network 10.2№.№.64   /26
 default-router 10.2№.№.X
 dns-server 8.8.8.8
```

После настройки DHCP сетевая карта PC2-Client переводится в режим автоматического приема ip-настроек.

Проверка: на PC2-Client должен открываться сайт cisco.com. На R1 в таблице маршрутизации должен присутствовать маршрут к сети PC2-Client, полученный через OSPF.

8. На R1 настраивается LAN-интерфейс (согласно дизайна).

```
description LAN_ASA5505
no shutdown
ip address 10.№.№.X   /28
```

Проверка: На R2 в таблице маршрутизации должен присутствовать маршрут к сети 10.№.№.128/28, полученный через OSPF.

9. Скрипт базовой настройки ASA5505.

```
conf t
hostname ASA5505
interface Ethernet0/0
 switchport access vlan 3
 exit
interface Ethernet0/1
 switchport access vlan 2
 exit
interface vlan 2
 nameif inside
 ip address 192.168.№.X /26
 exit
interface vlan 3
 nameif outside
 ip address 10.№.№.X /28
 exit
route outside 0.0.0.0 0.0.0.0 10.№.№.X 1
class-map global-class№
 match default-inspection-traffic
 exit
policy-map global_policy
 class global-class№
 inspect ftp
 inspect h323
 inspect http
 inspect icmp
 inspect tftp
 exit
service-policy global_policy global
object network inside-subnet
 subnet 192.168.№.0 /26
 nat (inside,outside) dynamic interface
exit
write memory
```

Настройка DHCP на ASA5505.

```
dhcpd address 192.168.№.X-192.168.№.X inside
dhcpd dns 8.8.8.8 interface inside
dhcpd enable inside
```

Настройка IP на LAN-устройствах.

На Intranet-server`e вручную применяются ip-настройки (согласно дизайна). PC1 получает ip-настройки по DHCP от ASA5505 (если есть проблемы с получением ip-адреса основного шлюза, то ip-настройки выполняются вручную).

Проверка: ping на 8.8.8.8 и 8.8.254.252 (cisco.com) должен проходить.

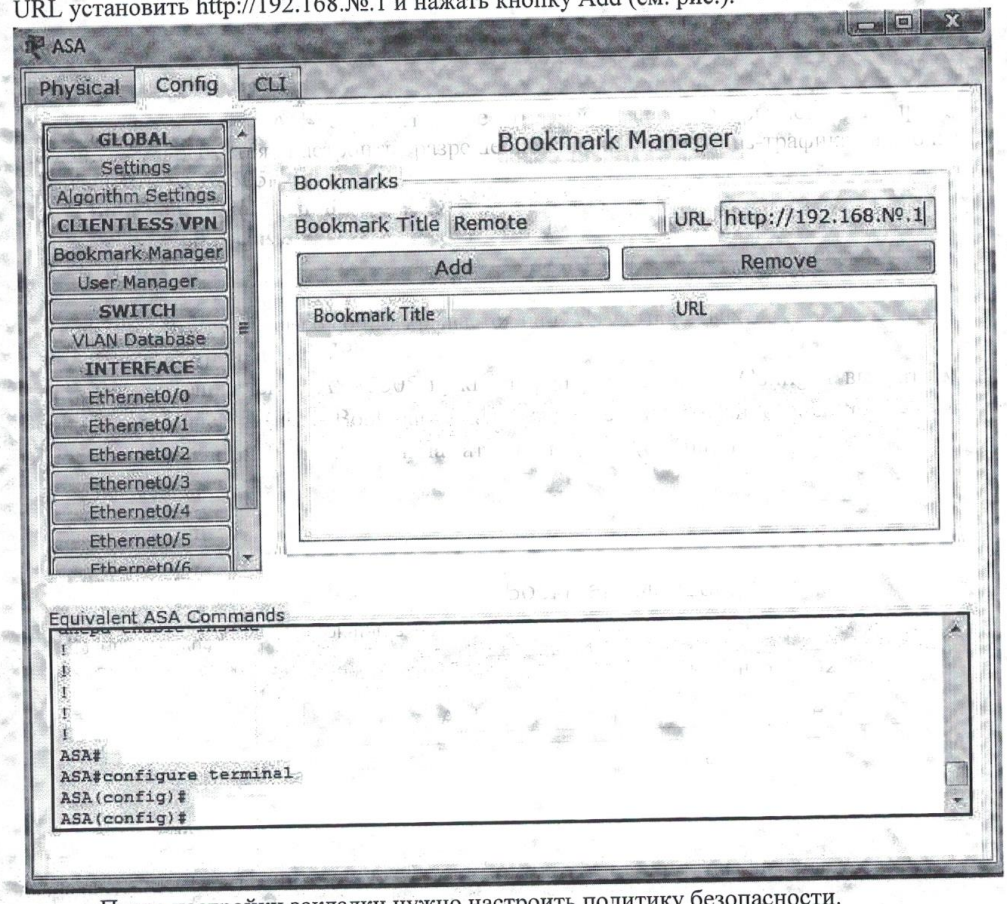
Cisco.com на LAN-устройствах не открывается, но открывается по ip-адресу 8.8.254.252. Требуется настроить разрешение прохождения dns-трафика в политике безопасности ASA5505.

policy-map global_policy
class global-class№
inspect dns
exit

Проверка: сайт cisco.com открывается на LAN-устройствах.

10. Настройка WebVPN.

В окне управления ASA5505 нужно перейти на вкладку Config и выбрать меню Bookmark Manager. В поле Bookmark Title нужно установить описание Remote, в поле URL установить http://192.168.№.1 и нажать кнопку Add (см. рис.).



После настройки закладки нужно настроить политику безопасности.

В режиме глобальной конфигурации включается webvpn и применяется на outside-интерфейс.

webvpn
enable outside
exit

Далее настраивается групповая политика удаленных пользователей.

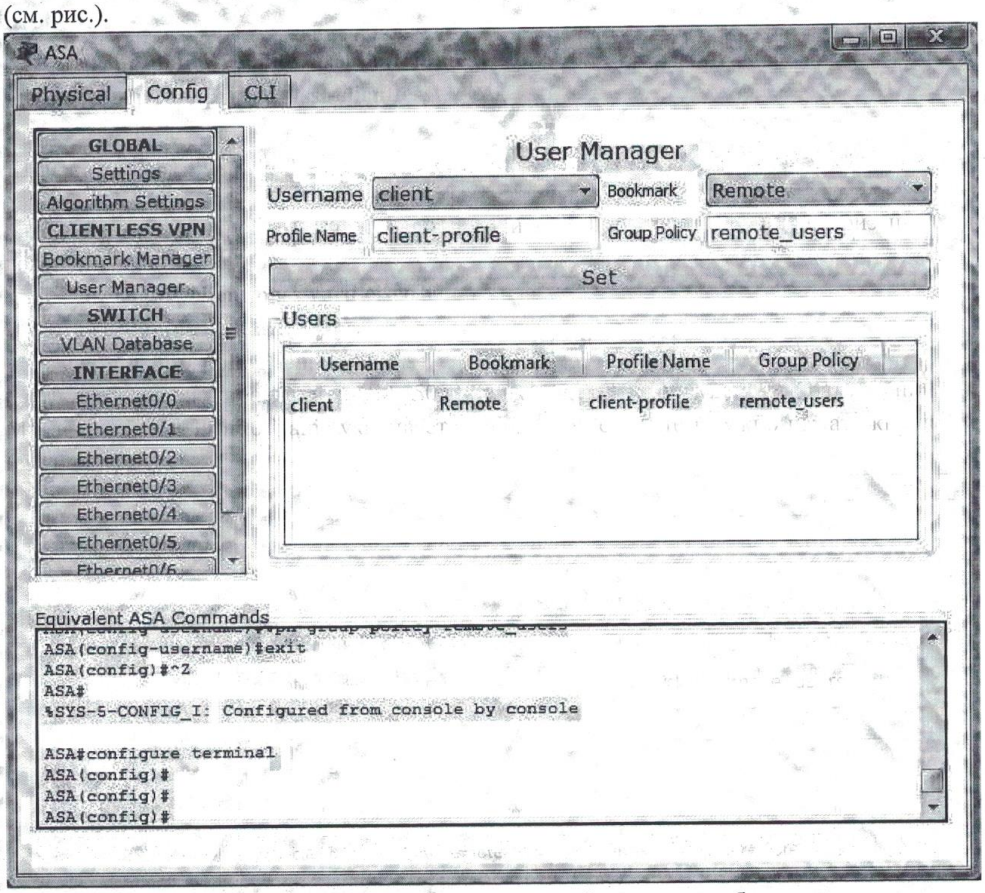
group-policy remote_users internal

group-policy remote_users attributes
vpn-tunnel-protocol ssl-clientless
webvpn
url-list value Remote
exit

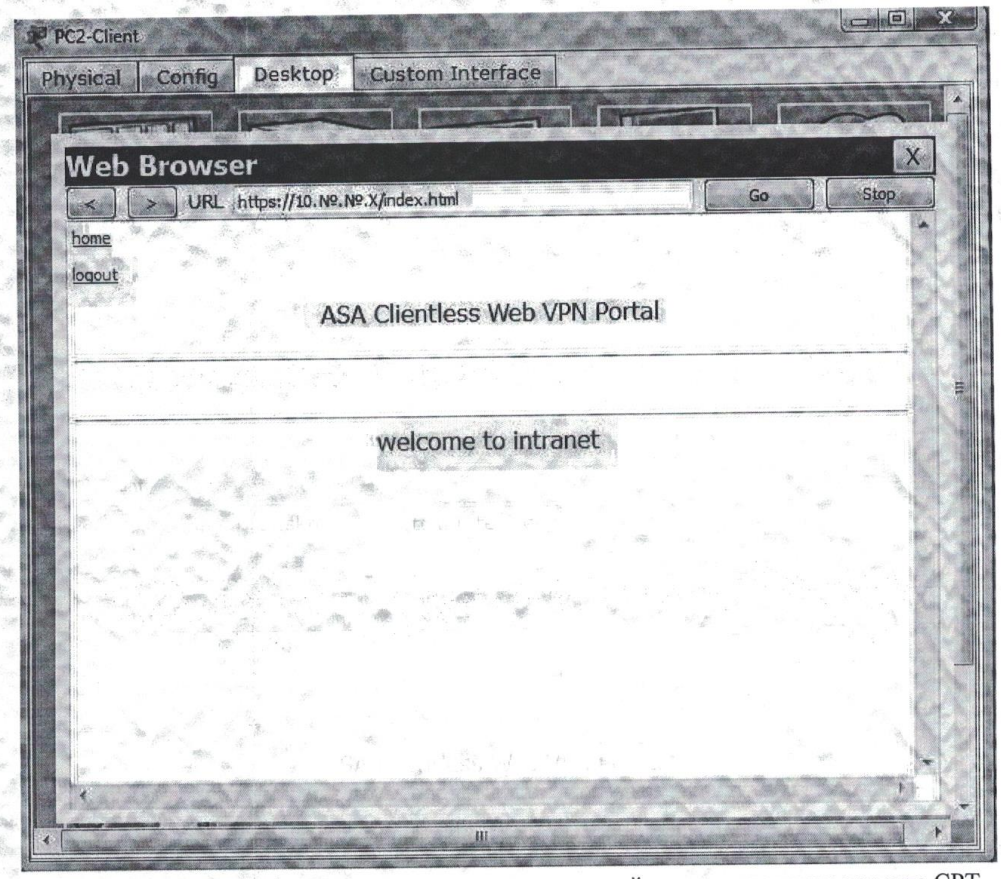
После настройки групповой политики настраивается авторизация по логину/паролю.

username client password cisco№
username client attributes
vpn-group-policy remote_users

На панели управления ASA5505 во вкладке Config нужно выбрать меню User Manager. В поле Profile Name указывается client-profile и затем нужно нажать кнопку Set (см. рис.).



Проверка: на PC2-Remote в адресной строке браузера указывается https://10.№.№.X (ip-адрес ASA5505, который назначен на outside-интерфейс). После установки соединения ASA5505 запросит логин/пароль. Если все выполнено правильно, то через защищенное соединение на PC2-Remote будет отправлена web-страница с Intranet-сервера (см. рис.).



Сохранение конфигурации на всех сетевых устройствах, сохранение проекта CPT.

Вопросы для входного контроля

1. Что такое брандмауэр в составе операционной системы?
2. Какая федеральная служба отвечает за защиту информации некриптографическими средствами?
3. Какими документами регламентируется необходимость использования межсетевых экранов в информационных системах?
4. Какими документами регламентируется необходимость использования систем обнаружения и предотвращения вторжений в информационных системах, имеющих подключение к сетям общего пользования и обрабатывающих информацию ограниченного доступа?
5. Каким образом можно обеспечить защиту информации при передаче ее за пределы контролируемого периметра организации?
6. Какими документами регламентируется обработка конфиденциальной информации и необходимость ее защиты?
7. Какими документами регламентируется обработка персональных данных и необходимость их защиты?
8. Каким документом регламентируется обработка информации в государственных информационных системах и необходимость ее защиты?
9. Перечислите необходимые составляющие для обеспечения защиты конфиденци-

альной информации при обработке ее на автономных автоматизированных рабочих местах.

10. Перечислите необходимые составляющие для обеспечения защиты конфиденциальной информации при обработке ее на рабочих местах подключенных к локальной вычислительной сети организации при отсутствии доступа к сетям общего пользования.
11. Перечислите необходимые составляющие для обеспечения защиты конфиденциальной информации при обработке ее на рабочих местах подключенных к локальной вычислительной сети организации при условии наличия доступа к сетям общего пользования.
12. При помощи каких механизмов можно разграничить доступ пользователей из одного сегмента локальной вычислительной сети к информации ограниченного доступа?
13. Что такое автоматизированная система?
14. Какие классы АС вы знаете?
15. Какие уровни защищенности информационных систем, обрабатывающих персональные данные вы знаете?
16. Какие классы государственных информационных систем вы знаете?

Контрольные вопросы к экзамену

1. Распределенная обработка данных.
2. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей.
3. Сетевые операционные системы.
4. Средства взаимодействия процессов в сетях.
5. Системы клиент-сервер, одноранговые сети, локальные и глобальные сети.
6. Маршрутизаторы, межсетевые экраны (МЭ). Основные схемы применения МЭ.
7. Абонентское шифрование. Виртуальные частные сети.
8. Идентификация и аутентификация абонентов сети.
9. Методы разделения ресурсов и технологии разграничения доступа.
10. Электронная цифровая подпись и пакетное шифрование.
11. Криптографические сетевые протоколы. Управление ключами.
12. Понятие политики сетевой безопасности. Типовые элементы политики сетевой безопасности.
13. Рекомендации по построению политики сетевой безопасности. Основные шаги по реализации политики сетевой безопасности.
14. Основные критерии анализа сетевой безопасности. Общая процедура анализа.
15. Модель OSI. Уязвимости базовых протоколов семейства TCP/IP и протоколов управления сетью.
16. Прикладные протоколы и службы. Защита от вирусов.
17. Особенности реализации и взаимодействия приложений на различных платформах.
18. Основные принципы обеспечения безопасности и управления распределенными ресурсами.
19. Обеспечение надежности инфраструктуры Интернет.
20. Виды используемых в Интернет каналов связи. Особенности их защиты.
21. Применение межсетевых экранов. Виртуальные частные сети.
22. Протоколы маршрутизации. Безопасность протоколов динамической маршрутизации.

23. Безопасность различных типов подключения к Интернет. Интеграция локальных сетей в региональные и глобальные сети.
24. Контроль и анализ обеспечения безопасности подключения к Интернет.
25. Сертифицированные средства анализа защищенности информационных систем
26. Регламент проведения проверок на наличие уязвимостей
27. Типовые схемы построения сетей предприятий с использованием межсетевых экранов
28. Типовые схемы построения сетей предприятий с использованием серверов доступа
29. Реестр сертифицированных средств защиты информации ФСТЭК
30. Порядок организации защиты при обработке конфиденциальной информации
31. Порядок организации защиты информации в информационных системах обрабатывающих персональные данные
32. Порядок организации защиты информации в государственных информационных системах
33. Обеспечение защиты информации при передаче за пределы контролируемой зоны
34. Сертифицированные средства криптографической защиты информации
35. Использование электронной и квалифицированной электронных подписей для обеспечения авторства информации, ее непротиворечивости
36. Основные возможности современных сканеров уязвимостей на примере XSpider
37. Основные возможности современных сканеров уязвимостей на примере Сканер-ВС
38. Несертифицированные системы анализа уязвимостей, на примере metasploit.
39. Аудит WiFi сетей, механизмы обеспечения их защиты.
40. Порядок организации работ по управлению системами защиты информации при использовании единого центра обеспечения информационной безопасности в организации на примере Dallas Lock
41. Порядок организации работ по управлению системами защиты информации при использовании единого центра обеспечения информационной безопасности в организации на примере Secret Net Studio.
42. Ведущие отечественные вендоры в сфере обеспечения информационной безопасности некрипографическими средствами в сетях ЭВМ
43. Ведущие отечественные вендоры в сфере обеспечения информационной безопасности с использованием средств криптографической защиты информации в сетях ЭВМ
44. Организация домена безопасности в сети на примере Dallas Lock
45. Организация домена безопасности в сети на примере Secret Net Studio
46. Технология защиты информации при трансграничной передаче.
47. Организация защиты информации штатными средствами оборудования на примере ACL, Vlan, протоколов маршрутизации.
48. Механизмы современных операционных систем для обеспечения информационной безопасности при функционировании в сети
49. Механизмы современных операционных систем для обеспечения информационной безопасности при функционировании в виртуальных инфраструктурах, и дата центрах.
50. Работа с отчуждаемыми носителями в сетях.

Типовые экзаменационные задачи

1. Разработайте схему защиты ЛВС предприятия 1 АРМ без доступа к сети.
2. Разработайте схему защиты ЛВС предприятия 1 АРМ без доступа к сети есть РСО.
3. Разработайте схему защиты ЛВС предприятия 1 АРМ есть интернет
4. Разработайте схему защиты ЛВС предприятия 1 АРМ есть РСО, есть доступ к интернет.
5. Разработайте схему защиты ЛВС предприятия несколько АРМ соединенных в ЛВС.
6. Разработайте схему защиты ЛВС предприятия несколько АРМ соединенных в ЛВС есть РСО нет подключения к интернет
7. Разработайте схему защиты ЛВС предприятия несколько АРМ соединенных в ЛВС есть РСО есть подключение к интернет
8. Разработайте схему защиты предприятия, состоящего из нескольких равноправных филиалов.
9. Разработайте схему защиты предприятия, состоящего из нескольких филиалов, доступ к головному офису осуществляется через сервер доступа.
10. Разработайте схему защиты предприятия, состоящего из нескольких неравноправных филиалов.

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
1	04.10.2021 протокол №2. Воспитательная работа обучающихся. Основание: *Федеральный закон от 31.07.2020 N 304-ФЗ "О внесении изменений в Федеральный закон "Об образовании в Российской Федерации" по вопросам воспитания обучающихся"*	1	
2	04.10.2021 протокол №2. Практическая подготовка обучающихся. Основание: *Приказ Министерства науки и высшего образования Российской Федерации, Министерства просвещения Российской Федерации от 05.08.2020 г. № 885/390 "О практической подготовке обучающихся"*	1	