

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ

по дисциплине «Персональная кибербезопасность»

для студентов направления подготовки

10.03.01 Информационная безопасность

Направленность (профиль)

«Организация и технологии защиты информации

(по отрасли или в сфере профессиональной деятельности)»

Ставрополь

2026

СОДЕРЖАНИЕ

Лабораторная работа № 1.	3
Тема: Кибербезопасность: мир специалистов и преступников Название задания:	
Создание кибермира	9
Учебный вопрос 1: Настройка FTP-сервера	10
Учебный вопрос 2: Настройка веб-сервера	10
Учебный вопрос 3: Настройка DNS-сервера	10
Учебный вопрос 4: Настройка сервера электронной почты	11
Учебный вопрос 5: Настройка NTP-сервера	12
Учебный вопрос 6: Настройка AAA-сервера	12
Лабораторная работа № 2.	14
Тема: Куб кибербезопасности Название задания: Общение в кибермире	14
Учебный вопрос 1: Передача электронного сообщения от пользователя к пользователю	15
Учебный вопрос 2: Загрузка файлов на сервер по протоколу FTP	15
Учебный вопрос 3: Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet	16
Учебный вопрос 4: Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH	17
Лабораторная работа № 3.	19
Тема: Свойства противодействия угрозам кибербезопасности Название задания:	
Шифрование файлов и данных	19
Учебный вопрос 1: Поиск данных учетной записи FTP для ноутбука пользователя Mary	20
Учебный вопрос 2: Загрузка конфиденциальных данных на сервер по протоколу FTP	20
Учебный вопрос 3: Поиск данных учетной записи FTP для компьютера пользователя Bob	21
Учебный вопрос 4: Загрузка конфиденциальных данных с сервера по протоколу FTP	21
Учебный вопрос 5: Расшифровка содержимого файла clientinfo.txt	22
Лабораторная работа № 4.	23

Тема: Угрозы кибербезопасности, уязвимости и атаки	Название задания: Проверка целостности файлов и данных	24
Учебный вопрос 1:	Загрузка файлов с информацией о клиентах на компьютер пользователя Mike	25
Учебный вопрос 2:	Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File	25
Учебный вопрос 3:	Проверка целостности файлов с информацией о клиентах с помощью хеширования	26
Учебный вопрос 4:	Проверка целостности критически важных файлов с помощью механизма HMAC	27
Лабораторная работа № 5.		30
Тема: Способы защиты информации ограниченного доступа	Название задания: WEP/WPA2 PSK/WPA2 RADIUS	30
Учебный вопрос 1:	Настройка WEP на объекте Healthcare at Home	31
Учебный вопрос 2:	Настройка WPA2 PSK на объекте Gotham Healthcare Branch.....	32
Учебный вопрос 3:	Настройка WPA2 RADIUS на объекте Metropolis Bank HQ	32
Предлагаемый способ подсчета баллов.....		34
Содержание отчета		34
Лабораторная работа № 6.		35
Тема: Способы обеспечения целостности данных	Название задания: Настройка транспортного режима VPN	35
Учебный вопрос 1:	Передача незашифрованного FTP-трафика	36
Учебный вопрос 2:	Настройка VPN-клиента на компьютере пользователя Phil	36
Учебный вопрос 3:	Передача зашифрованного FTP-трафика	37
Лабораторная работа № 7.		38
Тема: Концепция «пять девяток»	Название задания: Резервирование маршрутизаторов и коммутаторов	39
Учебный вопрос 1:	Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.	40
Учебный вопрос 2:	Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.	41

Лабораторная работа № 8.	43
Тема: Защита уровней обеспечения кибербезопасности Название задания: Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе	44
Учебный вопрос 1: Подключение к веб-серверу.	45
Учебный вопрос 2: Запрет незашифрованных сеансов HTTP.	45
Учебный вопрос 3: Доступ к межсетевому экрану на сервере электронной почты.	46
Лабораторная работа № 9.	47
Тема: Специалисты в области кибербезопасности. Название задания: Отработка комплексных практических навыков	48
Сценарий	48
Реализация	48

ВВЕДЕНИЕ

1. Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Персональная кибербезопасность» является получение базовых знаний и навыков, охватывающих все области кибербезопасности и информационной безопасности, системы безопасности, сетевую безопасность, безопасность мобильных устройств, физическую безопасность, этические и правовые требования, технологии и методы защиты и минимизации последствий в ходе обеспечения персональной кибербезопасности и информационной безопасности бизнеса.

Задачами дисциплины являются:

1. Ознакомление с миром кибербезопасности и мотивацией киберпреступников и специалистов по кибербезопасности.
2. Изучение этических требований и законов в области информационной безопасности и методов разработки политик безопасности.
3. Изучение функций специалистов по кибербезопасности и карьерных возможностей.
4. Получение фундаментальных знаний в различных областях безопасности.
5. Развитие умений, навыков и способностей определять кибератаки и их признаки, процессы и контрмеры информационной безопасности.
6. Приобретение навыков по управлению безопасностью, использованию средств контроля, защиты и технологий минимизации последствий.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Персональная кибербезопасность» относится к факультативам.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации (06.030 В)	ИД-3ПК-1 Способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	-формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, распределяет обязанности и полномочия персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, проверяет уровень квалификации персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, в том числе, при приеме на работу; - производит постановку задач персоналу по обеспечению защиты СССЭ

		от НСД и организует их выполнение, организует контроль выполнения организационно-технических мероприятий по обеспечению защиты СССЭ от НСД, организует перераспределение обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД; - усвоил цели и задачи по управлению персоналом, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, усвоил методику выбора и организации управленческих решений по обеспечению защиты сетей электросвязи от НСД, использует руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях. Способен администрировать средства защиты информации в компьютерных системах и сетях (06. 032 В)	ИД-2_{ПК-2} Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	- определяет состав программно-аппаратных средств защиты информации в компьютерных сетях, разрабатывает порядок применения программно-аппаратных средств защиты информации в компьютерных сетях, формирует шаблоны конфигураций программно-аппаратных средств защиты информации в компьютерных сетях; - оценивает угрозы безопасности информации в компьютерных сетях, настраивает правила фильтрации пакетов в компьютерных сетях, обосновывает выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; - понимает принципы построения компьютерных сетей, понимает порядок функционирования стека сетевых протоколов операционных систем, понимает принципы построения компьютерных сетей, понимает порядок функционирования стека протоколов сетевого оборудования
	ИД-3_{ПК-2} Способен администрировать средства защиты информации прикладного и системного программного обеспечения	- определяет порядок установки программного обеспечения с целью соблюдения требований по защите информации, контролирует соблюдение требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение, формулирует требования к параметрам средств антивирусной защиты для корректной работы программного обеспечения; - анализирует угрозы безопасности информации программного обеспечения, формулирует правила безопасной эксплуатации программного обеспечения,

		обосновывает правила безопасной эксплуатации программного обеспечения; - понимает архитектуру подсистем защиты информации в операционных системах, понимает принципы построения систем управления базами данных, понимает основные средства и методы анализа программных реализаций
--	--	---

Лабораторная работа № 1.

Тема: Кибербезопасность: мир специалистов и преступников

Название задания: Создание кибермира

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь настраивать базовые компоненты сервера.
3. Приобрести навыки развертывания служб FTP, электронной почты, DNS, NTP, AAA и веб-службы на нескольких серверах.
4. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Настройка FTP-сервера
2. Настройка веб-сервера
3. Настройка сервера электронной почты
4. Настройка DNS-сервера
5. Настройка NTP-сервера
6. Настройка сервера AAA

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения/сценарий

Выполняя это задание, вы настроите базовые компоненты сервера. Настройка IP-в соответствии с таблицей адресации. Пользуясь вкладкой Services (Службы), вы выполните развертывание служб FTP, электронной почты, DNS, NTP, AAA и веб-службы на нескольких серверах.

Таблица адресации

Устройство	IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	255.255.255.0	Metropolis Bank HQ
Сервер резервного копирования файлов	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Настройка FTP-сервера

Шаг 1: Активация службы FTP.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.
- b. Перейдите на вкладку **Services** (Службы) и выберите раздел **FTP**.
- c. Включите службу FTP с помощью селективной кнопки, которая находится в верхней части окна.

Шаг 2: Предоставьте пользователям доступ к FTP-серверу.

- a. Создайте учетные записи пользователей с именами **bob**, **mary** и **mike**, назначив каждой из них пароль **cisco123**.
- b. Каждая учетная запись должна иметь полные разрешения (RWDNL) на доступ к серверу FTP/Web.

Учебный вопрос 2: Настройка веб-сервера

Шаг 1: Активация службы HTTP.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.
- b. Перейдите на вкладку **Services** (Службы) и выберите **HTTP**.
- c. Включите службы HTTP и HTTPS с помощью селективных кнопок, которые находятся в верхней части окна.

Шаг 2: Проверка работоспособности службы HTTP.

- a. Выберите компьютер с именем "Sally" и перейдите на вкладку **Desktop** (Рабочий стол).
- b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.
- c. Пользуясь веб-браузером, перейдите по IP-адресу **10.44.1.254**.

Предположим, переход по IP-адресу происходит корректно, но при этом невозможно выполнить переход с использованием полного доменного имени. В чем может быть причина?

Учебный вопрос 3: Настройка DNS-сервера

Шаг 1: Активация службы DNS.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **Email/DNS**.
- b. Перейдите на вкладку **Services** (Службы) и выберите **DNS**.
- c. Включите службу DNS с помощью селективной кнопки в верхней части окна.

Шаг 2: Создание записей DNS A.

- a. Создайте запись **A email.cisco.corp** с IP-адресом **10.44.1.253**. Нажмите **Add** (Добавить), чтобы сохранить запись.
- b. Создайте запись **A www.cisco.corp** с IP-адресом **10.44.1.254**. Нажмите **Add** (Добавить), чтобы сохранить запись.

Шаг 3: Проверка работоспособности службы DNS.

- a. Выберите компьютер с именем "Sally" и перейдите на вкладку **Desktop** (Рабочий стол).
- b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.

Почему пользователь успешно переходит по указанному полностью квалифицированному имени домена?

Учебный вопрос 4: Настройка сервера электронной почты

Шаг 1: Активация сервисов электронной почты.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **Email/DNS**.
- b. Перейдите на вкладку **Services** (Службы) и выберите раздел **EMAIL** (Электронная почта).
- c. Включите службы **SMTP** и **POP3** с помощью селективных кнопок, которые находятся в верхней части окна.

Шаг 2: Создайте для пользователей учетные записи электронной почты.

- a. Создайте доменное имя **cisco.corp**.
- b. Создайте учетные записи пользователей с именами **phil, sally, bob, dave, mary, tim** и **mike**, назначив каждой учетной записи пароль **cisco123**.

Шаг 3: Настройка пользовательских клиентов электронной почты.

- a. Выберите компьютер с именем **Sally** и перейдите на вкладку **Desktop** (Рабочий стол).
- b. Щелкните значок **Email** (Электронная почта) и введите следующую информацию.

Name (Имя): **Sally**

Email Address (Адрес электронной почты): **sally@cisco.corp**

Incoming&OutgoingEmailServer(s) (сервер (-ы) входящей и исходящей почты):
email.cisco.corp

Username (имя пользователя): **sally**

Password (пароль): **cisco123**

- c. Повторите шаг **3b** на компьютере с именем **Bob**, заменив имя **sally** на **bob**.

Почему для работы сервиса электронной почты необходимо одновременно активировать службы SMTP и POP3?

Учебный вопрос 5: Настройка NTP-сервера

Шаг 1: Активация службы NTP.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.
- b. Перейдите на вкладку **Services** (Службы) и выберите **NTP**.
- c. Включите службу NTP с помощью селективной кнопки в верхней части окна.

Шаг 2: Защита службы NTP.

- a. Включите функцию аутентификации NTP с помощью соответствующей селективной кнопки.
- b. Назначьте ключу **Key 1** пароль **cisco123**.

Учебный вопрос 6: Настройка AAA-сервера

Шаг 1: Активация службы AAA.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.
- b. Перейдите на вкладку **Services** (Службы) и выберите **AAA**.
- c. Включите службу AAA с помощью селективной кнопки в верхней части окна.

Шаг 2: Сетевая конфигурация AAA.

- a. Введите имя Client Name (имя клиента) **HQ_Router**, адрес Client IP (IP-адрес клиента) **10.44.1.1** и пароль **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить параметры клиента.
- b. Настройте учетную запись пользователя AAA **admin** с паролем **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить информацию о пользователе.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 2. Настройка веб-сервера	Шаг 2	2	
Вопрос 3. Настройка DNS-сервера	Шаг 3	2	
Вопрос 4. Настройка сервера электронной почты	Шаг 3	2	
Вопросы		6	
Балл Packet Tracer		94	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Предположим, переход по IP-адресу происходит корректно, но при этом невозможно выполнить переход с использованием полного доменного имени. В чем может быть причина?
2. Почему пользователь успешно переходит по указанному полностью квалифицированному имени домена?
3. Почему для работы сервиса электронной почты необходимо одновременно активировать службы SMTP и POP3?

Лабораторная работа № 2.
Тема: Куб кибербезопасности
Название задания: Общение в кибермире

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь передавать электронные сообщения от пользователя к пользователю.
3. Приобрести навыки выгрузки файлов на сервер / с сервера по протоколу FTP.
4. Уметь осуществлять удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet.
5. Уметь осуществлять удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH.
6. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Передача электронных сообщений от пользователя к пользователю.
2. Выгрузка файлов на сервер / с сервера по протоколу FTP.
3. Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet.
4. Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH.

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения

Выполняя это задание, вы обеспечите общение через удаленные сети с помощью общих сетевых сервисов. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы будете пользоваться клиентскими устройствами, которые находятся в различных географических регионах. С этих устройств вы будете подключаться к другим клиентским устройствам и серверам.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Сервер резервного копирования файлов	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch
--------------------------------------	-------------	---	---------------	--------------------------

Учебный вопрос 1: Передача электронного сообщения от пользователя к пользователю

Шаг 1: Откройте клиент электронной почты на компьютере пользователя Mike.

- Откройте объект **Gotham Healthcare Branch** и выберите компьютер с именем **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

Шаг 2: Отправка электронного сообщения пользователю Sally.

- Нажмите кнопку **Compose** (Создать), чтобы создать электронное сообщение.
- В поле **To:** (Кому:) введите адрес sally@cisco.corp.
В поле **Subject:** (Тема:) введите текст "Urgent- Call me".
В поле **Message** (Сообщение) введите следующий текст. "Call me when you are free today to discuss the new sale."
- Нажмите кнопку **Send** (Отправить), чтобы отправить электронное сообщение.
По какому протоколу письмо было отправлено на сервер электронной почты?

Шаг 3: Проверка почты пользователем Sally.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер с именем **Sally**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
- Нажмите кнопку **Receive** (Получить), чтобы получить письмо, отправленное пользователем Mike.
По какому протоколу письмо было получено с сервера электронной почты?

Учебный вопрос 2: Загрузка файлов на сервер по протоколу FTP

Шаг 1: Настройка анализатора пакетов на перехват трафика соответствующего порта.

- Перейдите к географическому (корневому) виду, чтобы просмотреть все три удаленных объекта.
- Выберите анализатор трафика **Cyber Criminals Sniffer**.
- Выберите порт **Port1**, чтобы перехватывать пакеты на этом порте.
- Оставьте анализатор трафика **Cyber Criminals Sniffer** открытым и видимым до конца этой части работы.

Шаг 2: Удаленное подключение к FTP-серверу.

- Откройте объект **Healthcare at Home** и выберите компьютер с именем **Mary**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите команду **ftp 209.165.201.3** в командной строке.

- d. Введите имя пользователя **mary** и пароль **cisco123**.

Шаг 3: Загрузите файл на FTP-сервер.

- d. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- e. У пользователя Mary имеется файл с конфиденциальной информацией о новых клиентах медицинского учреждения.

Загрузите файл **newclients.txt** на FTP-сервер. Для этого введите команду **put newclients.txt**.

- f. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы убедиться в том, что файл **newclients.txt** теперь находится на FTP-сервере.

Почему загрузка по протоколу FTP считается небезопасным способом передачи файлов?

Шаг 4: Анализ FTP-трафика.

- a. Перейдите к географическому (корневому) виду, чтобы просмотреть все три удаленных объекта.
- b. Выберите анализатор трафика **Cyber Criminals Sniffer**.
- c. На вкладке GUI (Графический интерфейс) слева выберите первый доступный FTP-пакет. После этого полностью прокрутите вниз содержимое окна, отображаемого справа.

Какая информация из FTP-заголовка отображается в виде открытого текста?

- d. Слева выберите второй доступный FTP-пакет. После этого полностью прокрутите вниз содержимое окна, отображаемого справа. Повторите те же действия с третьим FTP-пакетом.
 - e. Какая конфиденциальная информация из FTP-заголовка (помимо имени пользователя) отображается в виде открытого текста?
-

Учебный вопрос 3: Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet

Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети.

- d. Откройте объект **Healthcare at Home** и выберите компьютер с именем **Dave**.
- e. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- f. Отправьте ring-запрос на маршрутизатор корпоративной сети, чтобы убедиться в наличии связи с маршрутизатором. Для этого введите команду **ping 209.165.201.2**.
- g. С помощью команды **telnet 209.165.201.2** установите соединение по протоколу Telnet с маршрутизатором корпоративной сети, которому назначен указанный IP-адрес.
- h. Выполните аутентификацию на маршрутизаторе корпоративной сети, используя имя пользователя **admin** и пароль **cisco123**.
- i. Введите команду **show users**, чтобы отобразить информацию об активном Telnet-соединении с маршрутизатором корпоративной сети.

Почему протокол Telnet считается небезопасным средством удаленного управления устройствами?

Учебный вопрос 4: Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH

Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети.

- a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер с именем **Tim**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- c. Отправьте ping-запрос на маршрутизатор корпоративной сети, чтобы убедиться в наличии связи с маршрутизатором. Для этого введите команду **ping 209.165.201.2**.
- d. С помощью команды **ssh -l admin 209.165.201.2** установите соединение по протоколу SSH с маршрутизатором корпоративной сети, которому назначен указанный IP-адрес.
- e. Выполните аутентификацию на маршрутизаторе корпоративной сети, используя пароль **cisco123**.
- f. Введите команду **show users**, чтобы отобразить информацию об активном SSH-соединении с маршрутизатором корпоративной сети.

Почему протокол SSH считается безопасным средством для удаленного управления устройствами?

-
- g. Перейдите в режим глобальной настройки. Для этого введите команду **configure terminal**.
 - h. С помощью команды **enable secret** создайте пароль **cisco**. Для этого введите команду **enable secret cisco**.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Передача электронных сообщений от пользователя к пользователю	Шаг 2	2	
	Шаг 3	2	
Вопрос 2. Выгрузка файлов на сервер /с сервера по протоколу FTP	Шаг 2	2	
	Шаг 3d	2	
	Шаг 3e	2	
Вопрос 3. Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet	Шаг 1	2	
Вопрос 4. Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH	Шаг 1	2	
Вопросы		14	
Балл Packet Tracer		86	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. По какому протоколу письмо отправляется на сервер электронной почты??
2. По какому протоколу письмо принимается с сервера электронной почты?
3. Почему загрузка по протоколу FTP считается небезопасным способом передачи файлов?
4. Какая информация из FTP-заголовка отображается в виде открытого текста?
5. Какая конфиденциальная информация из FTP-заголовка (помимо имени пользователя) отображается в виде открытого текста?
6. Почему протокол SSH считается безопасным средством для удаленного управления устройствами?

Лабораторная работа № 3.

Тема: Свойства противодействия угрозам кибербезопасности

Название задания: Шифрование файлов и данных

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь осуществлять поиск данных учетной записи FTP.
3. Уметь осуществлять выгрузку конфиденциальных данных на сервер по протоколу FTP.
4. Уметь осуществлять загрузку конфиденциальных данных на сервер по протоколу FTP.
5. Приобрести навыки расшифровки содержимого файла.
6. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Поиск данных учетной записи FTP для ноутбука пользователя Mary.
2. Выгрузка конфиденциальных данных на сервер по протоколу FTP.
3. Поиск данных учетной записи FTP для компьютера пользователя Bob.
4. Загрузка конфиденциальных данных с сервера по протоколу FTP.
5. Расшифровка содержимого файла clientinfo.txt.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы получите доступ к зашифрованному содержимому нескольких файлов и передадите файл через Интернет на центральный FTP-сервер. Затем другой пользователь загрузит файл с FTP-сервера и расшифрует содержимое файла. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Пользуясь клиентскими устройствами, которые находятся в различных географических регионах, вы передадите файл с зашифрованными данными с одного устройства на другое.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Mary	10.44.3.101	—	255.255.255.0	Healthcare at Home
Боб	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Поиск данных учетной записи FTP для ноутбука пользователя Mary

Шаг 1: Получение доступа к текстовому документу на ноутбуке пользователя Mary.

- Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- Выберите документ **ftplogin.txt** и нажмите кнопку **OK**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Mary.

- Выделите весь текст, содержащийся в файле **ftplogin.txt**, и скопируйте его.
- Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт <https://encipher.it>.
- Поместите курсор в белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст.

Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки **maryftp123**. Нажмите **Decrypt** (Расшифровать).

Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Mary?

Учебный вопрос 2: Загрузка конфиденциальных данных на сервер по протоколу FTP

Шаг 1: Просмотр конфиденциального документа на ноутбуке пользователя Mary.

- Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- Выберите документ **clientinfo.txt** и нажмите кнопку **OK**.

В какой форме представлены данные?

Шаг 2: Удаленное подключение к FTP-серверу.

- Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.

- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите команду **ftp 209.165.201.3** в командной строке.
- d. Введите имя пользователя и пароль, найденные на Шаге 2 в Части 1.

Шаг 3: Загрузите файл на FTP-сервер.

- a. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- b. У пользователя Mary имеется файл с зашифрованной информацией о клиентах медицинского учреждения. Загрузите файл **clientinfo.txt** на FTP-сервер. Для этого введите команду **put clientinfo.txt**.
- c. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы убедиться в том, что файл **clientinfo.txt** находится на FTP-сервере.

Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?

Учебный вопрос 3: Поиск данных учетной записи FTP для компьютера пользователя Bob

Шаг 1: Получение доступа к текстовому документу на компьютере пользователя Bob.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- d. Выберите документ **ftplogin.txt** и нажмите кнопку **OK**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Bob.

- a. Выделите весь текст, содержащийся в файле **ftplogin.txt**, и скопируйте его.
- b. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт <https://encipher.it>.
- c. Поместите курсор в белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст.
- d. Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки **bobftp123**. Нажмите **Decrypt** (Расшифровать).

Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Bob?

Учебный вопрос 4: Загрузка конфиденциальных данных с сервера по протоколу FTP

Шаг 1: Удаленное подключение к FTP-серверу.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

- c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите в командной строке команду **ftp 10.44.1.254**.
- d. Введите имя пользователя и пароль, найденные на Шаг 2 в Части 3.

Шаг 2: Загрузите файл на компьютер пользователя Bob.

- a. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- b. Пользователь Mary загрузила на сервер файл **clientinfo.txt** с зашифрованной информацией о клиентах медицинского учреждения.

Загрузите файл **clientinfo.txt** на компьютер пользователя Bob. Для этого введите команду **get clientinfo.txt**.

- c. В командную строку с подсказкой **ftp>** введите команду **quit**.
- d. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что файл **clientinfo.txt** находится на компьютере пользователя Bob.

Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?

Учебный вопрос 5: Расшифровка содержимого файла **clientinfo.txt**

Шаг 1: Получение ключа расшифровки от пользователя Mary.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
- c. В окне приложения Email (Электронная почта) нажмите кнопку **Receive** (Получить).
- d. Выберите электронное сообщение с темой "Decryption Key" («Ключ расшифровки») и запишите ключ расшифровки ниже.

Какой ключ расшифровки необходим для доступа к конфиденциальной информации, содержащейся в файле **clientinfo.txt**?

Шаг 2: Расшифровка содержимого файла **clientinfo.txt**.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- d. Выберите документ **clientinfo.txt** и нажмите кнопку **OK**.
- e. Выделите весь текст, содержащийся в файле **clientinfo.txt**, и скопируйте его.
- f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт <https://encipher.it>.
- g. Поместите курсор в белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст.

Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки, полученный в электронном сообщении от пользователя Mary. Нажмите **Decrypt** (Расшифровать).

Каково имя первой учетной записи в файле **clientinfo.txt**?

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Поиск данных учетной записи FTP для ноутбука пользователя Mary	Шаг 2	2	
Вопрос 2. Выгрузка конфиденциальных данных на сервер по протоколу FTP	Шаг 1	2	
	Шаг 3	2	
Вопрос 3. Поиск данных учетной записи FTP для компьютера пользователя Bob	Шаг 2	2	
Вопрос 4. Загрузка конфиденциальных данных с сервера по протоколу FTP	Шаг 2	2	
Вопрос 5. Расшифровка содержимого файла clientinfo.txt	Шаг 1	2	
	Шаг 2	2	
Вопросы		14	
Балл Packet Tracer		86	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Mary?
2. Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?
3. Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Bob?
4. Какой ключ расшифровки необходим для доступа к конфиденциальной информации, содержащейся в файле clientinfo.txt?
5. Каково имя первой учетной записи в файле clientinfo.txt?

Лабораторная работа № 4.

Тема: Угрозы кибербезопасности, уязвимости и атаки

Название задания: Проверка целостности файлов и данных

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь проверять целостность файлов с помощью хеширования.
3. Приобрести навыки проверки целостности критически важных файлов с помощью механизма HMAC.

Учебные вопросы занятия

1. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike.
2. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File.
3. Проверка целостности файлов с информацией о клиентах с помощью хеширования.
4. Проверка целостности критически важных файлов с помощью механизма HMAC.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы будете проверять целостность файлов с помощью хеш-сумм, чтобы убедиться в том, что содержимое файлов не было искажено. Файлы, целостность которых вызовет сомнение, следует передать на компьютер пользователя Sally для дальнейшего анализа. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы будете проверять и пересылать подозрительные файлы с помощью клиентских устройств, которые находятся в различных географических регионах.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Резервный файловый сервер Backup File	—	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Интернет

Mike	10.44.2.101	—	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	—	255.255.255.0	Metropolis Bank HQ
Боб	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike

Шаг 1: Получение доступа к FTP-серверу с компьютера пользователя Mike.

- Откройте объект **GothamHealthcare Branch** и выберите компьютер с именем **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- Введите URL-адрес **http://www.cisco.corp** и нажмите кнопку **Go** (Перейти).
- Перейдите по ссылке, чтобы загрузить новейшие версии файлов.

По какому протоколу был предоставлен доступ к этой веб-странице на резервном файловом сервере Backup File?

Шаг 2: Файловый сервер взломан. Об этом необходимо уведомить пользователя Sally.

- Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
- Создайте электронное сообщение с сообщением о взломе файлового сервера и отправьте это письмо на адрес Sally@cisco.corp.

Учебный вопрос 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File

Шаг 1: Получение доступа к внешнему FTP-серверу с компьютера пользователя Mike.

- Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).
- Перейдите по ссылке, чтобы просмотреть список новейших файлов и соответствующих хеш-сумм.

По какому протоколу был предоставлен доступ к этой веб-странице на резервном файловом сервере Backup File?

Каковы имена и хеш-суммы файлов на резервном файловом сервере?

Шаг 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike.

- Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.
- Введите имя пользователя **mike** и пароль **cisco123**.
- В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- Загрузите шесть файлов с информацией о клиентах (**NEclients.txt**, **NWclients.txt**, **Nclients.txt**, **SEclients.txt**, **SWclients.txt**, **Sclients.txt**) на компьютер пользователя Mike с помощью команды **get FILENAME.txt**, где "FILENAME" — имя загружаемого файла.

```
ftp>get NEclients.txt
```

Чтение файла NEclients.txt с www.cisco2.corp:

File transfer in progress...

[Передача завершена — 584 байта]

584 bytes copied in 0.05 secs (11680 bytes/sec)

- Загрузив все файлы, введите команду **quit** в командную строку с подсказкой **ftp>**.
- В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что файлы с информацией о клиентах действительно находятся на компьютере пользователя Mike.

Учебный вопрос 3: Проверка целостности файлов с информацией о клиентах с помощью хеширования

Шаг 1: Проверка хеш-сумм на компьютере пользователя Mike.

- Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- Выберите документ **NEclients.txt** и нажмите кнопку **OK**.
- Полностью скопируйте содержимое текстового документа.
- Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://www.tools4noobs.com/online_tools/hash/.
- Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Убедитесь в том, что выбран алгоритм md2. Нажмите кнопку **Hash this!** (Вычислить хеш-сумму).
- Чтобы удостовериться в том, что содержимое файла не было искажено, сравните полученную хеш-сумму с соответствующей хеш-суммой из списка файлов, который вы получили на шаге 1 в части 2.
- Повторите шаги d–h для каждого файла с информацией о клиентах и сравните полученные хеш-суммы с первоначальными хеш-суммами из списка файлов, который вы получили на шаге 1 в части 2.

Какой из файлов имеет некорректную хеш-сумму (то есть был искажен)?

Шаг 2: Загрузка подозрительного файла на компьютер пользователя Sally.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.
- Введите имя пользователя **sally** и пароль **cisco123**.
- В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- Загрузите с сервера искаженный файл, выявленный на шаге 1 в части 3.
- В командную строку с подсказкой **ftp>** введите команду **quit**.
- В командную строку с подсказкой **PC>** введите команду **dir**, чтобы удостовериться в том, что искаженный файл успешно загружен на компьютер пользователя Sally для последующего анализа.

Учебный вопрос 4: Проверка целостности критически важных файлов с помощью механизма HMAC

Шаг 1: Расчет HMAC-суммы критически важного файла.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что критически важный файл **income.txt** находится на компьютере пользователя Bob.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- Выберите документ **income.txt** и нажмите кнопку **OK**.
- Полностью скопируйте содержимое текстового документа.
- Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт <http://www.freeformatter.com/hmac-generator.html>.
- Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Введите секретный ключ **cisco123**. Убедитесь в том, что выбран алгоритм **SHA1**. Нажмите кнопку **Compute HMAC** (Рассчитать HMAC).
Какова HMAC-сумма содержимого файла?

Почему механизм HMAC безопаснее обычного хеширования?

Шаг 2: Проверьте полученную HMAC-сумму.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).
- Перейдите по ссылке, чтобы просмотреть список новейших файлов и соответствующих хеш-сумм.

Совпадает ли полученная хеш-сумма HMAC файла income.txt с хеш-суммой в списке?

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike	Шаг 1	2	
Вопрос 2. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File	Шаг 1	2	
	Шаг 1	6	
Вопрос 3. Проверка целостности файлов с информацией о клиентах с помощью хеширования	Шаг 1	5	
Вопрос 4. Проверка целостности критически важных файлов с помощью механизма HMAC	Шаг 1	5	
	Шаг 1	5	
	Шаг 2	5	
Вопросы		30	
Балл Packet Tracer		70	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. По какому протоколу был предоставлен доступ к веб-странице на резервном файловом сервере Backup File?
2. Каковы имена и хеш-суммы файлов на резервном файловом сервере?
3. Какой из файлов имеет некорректную хеш-сумму (то есть был искажен)?
4. Какова HMAC-сумма содержимого файла?
5. Почему механизм HMAC безопаснее обычного хеширования?
6. Совпадает ли полученная хеш-сумма HMAC файла income.txt с хеш-суммой

в списке?

Лабораторная работа № 5.

Тема: Способы защиты информации ограниченного доступа

Название задания: WEP/WPA2 PSK/WPA2 RADIUS

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь настраивать WEP на объекте.
3. Уметь настраивать WPA2 PSK на объекте.
4. Уметь настраивать WPA2 RADIUS.
5. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Настройка WEP на объекте Healthcare at Home.
2. Настройка WPA2 PSK на объекте Gotham Healthcare Branch.
3. Настройка WPA2 RADIUS на объекте Metropolis Bank HQ.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы настроите сети Wi-Fi на всех трех объектах. В этом упражнении вы будете работать с защитой WEP, WPA2 PSK и WPA2 RADIUS. Таким образом, вы познакомитесь с различными конфигурациями сетей Wi-Fi и особенностями обеспечения их безопасности. На объекте Healthcare at Home вы настроите защиту WEP. На объектах Gotham Healthcare Branch и Metropolis Bank HQ нужно будет настроить защиту WPA2 PSK и WPA2 Radius соответственно. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы настроите несколько безопасных беспроводных сетей, пользуясь беспроводными маршрутизаторами и клиентскими устройствами, которые находятся в различных географических регионах.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Настройка WEP на объекте Healthcare at Home

Шаг 1: Настройка идентификатора SSID беспроводной сети.

- a. Откройте объект **Healthcare at Home** и выберите **PC0**.
- b. Выберите вкладку **Desktop**. Щелкните **Командная строка**. Введите в командную строку команду **ipconfig**.

PC>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::20B:BEFF:FEB4:1262

IP Address.....: 10.44.3.100

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 10.44.3.1

Какой IP-адрес назначен шлюзу по умолчанию?

-
- c. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес шлюза по умолчанию. Введите **admin** в качестве имени пользователя и пароля. Щелкните **OK**.
 - d. В этой сетевой инфраструктуре шлюзом по умолчанию является беспроводной маршрутизатор **Wireless Router**. Перейдите на вкладку **Wireless** (Беспроводная сеть).
 - e. Измените идентификатор **SSID** с **DefaultWIFI** на **Home**.
 - f. Включите передачу идентификатора **SSID**. Для этого выберите вариант **Broadcast** (Передавать).
 - g. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

- a. Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **WirelessSecurity** (Защита беспроводной сети).
- b. В раскрывающемся меню **Security Mode** (Режим защиты) выберите **WEP**.
- c. Параметр **Encryption** (Шифрование) имеет значение по умолчанию 40/64-bits (40/64 бита). Не меняйте это значение. В качестве ключа **Key 1** введите **0123456789**.
- d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Защита WEP и ключ 0123456789 ненадежны. Почему алгоритм WEP считается недостаточно безопасным?

Шаг 3: Подключение клиентских устройств.

- a. Откройте объект **Healthcare at Home** и выберите ноутбук **Dave**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).
- c. Перейдите на вкладку **Connect** (Подключиться) и нажмите кнопку **Refresh** (Обновить).
- d. Выберите название беспроводной сети **Home** и нажмите кнопку **Connect** (Подключиться).
- e. В качестве ключа **WEP Key 1** введите ключ **0123456789** и нажмите кнопку **Connect** (Подключиться).
- f. Повторите шаги **a–e** на ноутбуке **Mary**.

Учебный вопрос 2: Настройка WPA2 PSK на объекте Gotham Healthcare Branch

Шаг 1: Настройка идентификатора SSID беспроводной сети.

- a. Откройте объект **Gotham Healthcare Branch** и выберите **PC1**.
- b. Выберите вкладку **Desktop**. Щелкните **Командная строка**. Введите в командную строку команду **ipconfig**.
Запишите IP-адрес шлюза по умолчанию.

- c. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес шлюза по умолчанию. Введите **admin** в качестве имени пользователя и пароля. Щелкните **OK**.
- d. Перейдите на вкладку **Wireless** (Беспроводная сеть).
- e. Измените идентификатор **SSID** с **DefaultWIFI** на **BranchSite**.
- f. Измените значение параметра **Standard Channel** (Стандартный канал) на **6 — 2.437GHz**.
- g. Включите передачу идентификатора **SSID**. Для этого выберите вариант **Broadcast** (Передавать).
- h. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

- a. Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **WirelessSecurity** (Защита беспроводной сети).
- b. В раскрывающемся меню **Security Mode** (Режим защиты) выберите **WPA2 Personal**.
- c. Параметр **Encryption** по умолчанию имеет значение **AES**. Не меняйте это значение. В качестве фразы-пароля введите **ciscosecure**.
- d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Подключение клиентских устройств.

- a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Tim**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).
- c. Перейдите на вкладку **Connect** (Подключиться) и нажмите кнопку **Refresh** (Обновить).
- d. Выберите название беспроводной сети **BranchSite** и нажмите кнопку **Connect** (Подключиться).
- e. Введите PSK-ключ **ciscosecure** и нажмите кнопку **Connect** (Подключиться).
- f. Повторите шаги **a–e** на компьютере **Mike**.

Учебный вопрос 3: Настройка WPA2 RADIUS на объекте Metropolis Bank HQ

Шаг 1: Настройка идентификатора SSID беспроводной сети.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.
- b. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес беспроводного маршрутизатора (**10.44.1.251**). Введите **admin** в качестве имени пользователя и пароля. Щелкните **OK**.
- c. Перейдите на вкладку **Wireless**. Измените идентификатор **SSID** с **DefaultWIFI** на **HQ**.
- d. Измените значение параметра **Standard Channel** (Стандартный канал) на **11 — 2.462GHz**.

- e. Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).
- f. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

- a. Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **WirelessSecurity** (Защита беспроводной сети).
- b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2-Enterprise**.
- c. Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. Введите следующие параметры сервера RADIUS:

RADIUSSERVERIP (IP-адрессервераRADIUS): **10.44.1.252**

Shared Secret (Общийсекретныйключ): **ciscosecure**
- d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Настройка сервера RADIUS.

- a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.
- b. Перейдите на вкладку **Services** (Службы) и выберите раздел **AAA**.
- c. Введите следующую информацию в области **Network Configuration** (Конфигурация сети):

Client Name (Имя клиента):.....**HQ**

Client IP (IP-адрес клиента):.....**10.44.1.251**

Secret (Ключ):..... **ciscosecure**

ServerType (Типсервера):.....**Radius**
- d. Нажмите **Добавить**.
- e. Введите указанные ниже данные в области **User Setup** (Параметры пользователей) и нажмите кнопку **Add** (Добавить), чтобы добавить новое имя пользователя.

Username (Имя пользователя): **bob** Password (Пароль): **secretninjabob**

Username (Имя пользователя): **phil** Password (Пароль): **philwashere**

Шаг 4: Подключение клиентских устройств.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).
- c. Перейдите на вкладку **Profiles** (Профили) и нажмите кнопку **New** (Создать).
- d. Введите имя профиля **RADIUS** и нажмите кнопку **OK**.
- e. Нажмите **Advanced Setup** (Расширенная настройка).
- f. В поле Wireless Network Name (Название беспроводной сети) введите **HQ** и нажмите **Next** (Далее).
- g. Не меняя сетевые настройки, вновь нажмите **Next** (Далее).
- h. В раскрывающемся меню Wireless Security (Режим защиты) выберите **WPA2-Enterprise** и нажмите **Next** (Далее).
- i. Введите имя пользователя **bob** и пароль **secretninjabob**. Нажмите **Next** (Далее).
- j. Нажмите **Save** (Сохранить), затем нажмите **Connect to Network** (Подключиться к сети).
- k. Подключение компьютера **Bob** будет выполнено автоматически.

1. Повторите шаги **a–j** на ноутбуке **Phil**, используя аутентификационную информацию, указанную в описании шага 3e.

Почему в крупной организации разумнее применить режим WPA2 RADIUS вместо WPA2 PSK?

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Настройка WEP на объекте Healthcare at Home	Шаг 2	5	
Вопрос 3. Настройка WPA2 RADIUS на объекте Metropolis Bank HQ	Шаг 4	5	
Вопросы		10	
Балл Packet Tracer		90	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какой IP-адрес назначен шлюзу по умолчанию?
2. Защита WEP и ключ 0123456789 ненадежны. Почему алгоритм WEP считается недостаточно безопасным?
3. Запишите IP-адрес шлюза по умолчанию.
4. Почему в крупной организации разумнее применить режим WPA2 RADIUS вместо WPA2 PSK?

Лабораторная работа № 6.

Тема: Способы обеспечения целостности данных Название задания: Настройка транспортного режима VPN

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь передавать незашифрованный FTP-трафик.
3. Уметь передавать зашифрованный FTP-трафик.
4. Приобрести способность настраивать VPN-клиента на объекте.
5. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Передача незашифрованного FTP-трафика.
2. Настройка VPN-клиента на объекте Metropolis.
3. Передача зашифрованного FTP-трафика.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы будете отслеживать передачу незашифрованного FTP-трафика между клиентом и удаленным объектом. Затем вы настроите VPN-клиент для подключения к объекту Gotham Healthcare Branch и начнете передачу зашифрованного FTP-трафика. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Передачу зашифрованных и незашифрованных FTP-данных вы будете выполнять с помощью клиентского устройства, которое находится в пределах объекта Metropolis Bank HQ.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Private_FTP server	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch
Public_FTP server	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	—	209.165.201.19	255.255.255.248	Gotham Healthcare Branch

Компьютер Phil's	10.44.0.2	—	255.255.255.0	Metropolis Bank HQ
------------------	-----------	---	---------------	--------------------

Учебный вопрос 1: Передача незашифрованного FTP-трафика

Шаг 1: Получение доступа к анализатору трафика Cyber Criminals Sniffer.

- Выберите анализатор трафика **Cyber Criminals Sniffer** и перейдите на вкладку **GUI** (Графический интерфейс).
- Нажмите кнопку **Clear** (Очистить), чтобы удалить все собранные ранее записи с информацией о трафике.
- Сверните окно анализатора трафика **Cyber Criminals Sniffer**.

Шаг 2: Установите небезопасное FTP-соединение с сервером Public_FTP.

- Откройте объект **Metropolis Bank HQ** и выберите ноутбук **Phil**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **Command Prompt** (Командная строка).
- Введите команду **ipconfig**, чтобы отобразить текущий IP-адрес компьютера **Phil**.
- Установите соединение с сервером **Public_FTP** объекта **Gotham Healthcare Branch**. Для этого введите в командную строку команду **ftp 209.165.201.20**.
- Введите имя пользователя **cisco** и пароль **publickey**, чтобы войти на сервер **Public_FTP**.
- С помощью команды **put** выгрузите файл **PublicInfo.txt** на сервер **Public_FTP**.

Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer.

- Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.
- В анализаторе трафика выберите сообщения **FTP** и полностью прокрутите содержимое каждого из сообщений.
Какая информация отображается в виде открытого текста?

- Введите **quit**, чтобы завершить сеанс на сервере **Public_FTP**.

Учебный вопрос 2: Настройка VPN-клиента на компьютере пользователя Phil

- На компьютере **Phil's** выполните команду **ping**, указав IP-адрес маршрутизатора **Branch_Router**. Первые несколько **ping**-запросов могут остаться без ответа из-за превышения времени ожидания. Введите команду **ping**. Вы должны получить ответы на четыре **ping**-запроса.
- Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **VPN**.
- В окне **VPN Configuration** (Настройка VPN) введите следующие параметры:
 GroupName (Имя группы):..... **VPNGROUP**
 Group Key (Ключ группы):..... **123**
 Host IP (Server IP) (IP-адрес хоста (IP-адрес сервера)):..... **209.165.201.19**
 Username (Имя пользователя):..... **phil**
 Password (Пароль):..... **cisco123**
- Нажмите кнопку **Connect** (Подключиться) и затем кнопку **OK** в следующем окне.

Какой IP-адрес клиента применяется для установки VPN-соединения «клиент-объект»?

Учебный вопрос 3: Передача зашифрованного FTP-трафика

Шаг 1: Просмотр текущих параметров IP-адресации на компьютере пользователя Phil.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Phil**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **Command Prompt** (Командная строка).
- С помощью команды **ipconfig** отобразите текущий IP-адрес компьютера **Phil**.

Видите ли вы дополнительный IP-адрес, который не отображался ранее на шаге 2с в части 1? Какой это адрес?

Шаг 2: Передача зашифрованного FTP-трафика с компьютера пользователя Phil на сервер Private_FTP.

- Установите соединение с сервером **Private_FTP** объекта **Gotham Healthcare Branch**. Для этого введите команду **ftp 10.44.2.254** в командную строку.
- Введите имя пользователя **cisco** и пароль **secretkey**, чтобы войти на сервер **Private_FTP**.
- Выгрузите файл **PrivateInfo.txt** на сервер **Private_FTP**.

Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer

- Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.
- Выберите сообщения **FTP** в окне анализатора трафика.

Есть ли среди них FTP-сообщения, в которых отображается внутренний пароль или информация о выгрузке файла PrivateInfo.txt на сервер? Дайте пояснение.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Передача незашифрованного FTP-трафика	Шаг 3	20	
Вопрос 2. Настройка VPN-клиента на компьютере пользователя Phil	Шаг 1	10	
Вопрос 3. Передача зашифрованного FTP-трафика	Шаг 1	10	
	Шаг 3	20	
Вопросы		60	
Балл Packet Tracer		40	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какая информация отображается в виде открытого текста?
2. Какой IP-адрес клиента применяется для установки VPN-соединения «клиент-объект»?
3. Видите ли вы дополнительный IP-адрес, который не отображался ранее на шаге 2с в части 1? Какой это адрес?
4. Есть ли среди FTP-сообщений FTP-сообщения, в которых отображается внутренний пароль или информация о выгрузке файла PrivateInfo.txt на сервер? Дайте пояснение

Лабораторная работа № 7.

Тема: Концепция «пять девяток»

Название задания: Резервирование маршрутизаторов и коммутаторов

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Приобрести способность наблюдения за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.
3. Приобрести способность наблюдения за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.
4. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.
2. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

В этом задании вы будете наблюдать за успешным переключением при отказе сетевой инфраструктуры Metropolis. Для резервирования шлюза по умолчанию используются несколько маршрутизаторов. Затем будет проведено успешное переключение при отказе сетевой инфраструктуры Gotham. Резервирование сетевых маршрутов будет обеспечиваться с помощью нескольких коммутаторов. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Для тестирования маршрутов до и после успешного переключения при отказе сетевой инфраструктуры вы будете использовать клиентские устройства в различных географических регионах.

Таблица адресации

Устройство	IP-адрес	Маска подсети	Шлюз по умолчанию	Сайт
Внешний веб-сервер	209.165.201.10	255.255.255.0	—	Интернет
R1	10.44.1.2	255.255.255.0	—	Metropolis Bank HQ
R2	10.44.1.3	255.255.255.0	—	Metropolis Bank HQ
Компьютер Phil's	10.44.1.12	255.255.255.0	10.44.1.1	Metropolis Bank HQ

Компьютер Tim's	10.44.2.11	255.255.255.0	10.44.2.1	Gotham Healthcare Branch
-----------------	------------	---------------	-----------	--------------------------

Учебный вопрос 1: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.

Шаг 1: Откройте командную строку на компьютере пользователя Phil.

- Выберите узел **Metropolis Bank HQ** и выберите ноутбук **Phil**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Проследите маршрут к внешнему веб-серверу.

- Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.
- Проследите маршрут к серверу **External Web** в **Интернете**. Для этого в командной строке введите **tracert 209.165.201.10**.
- IP-адреса в выводе команды **tracert** представляют сетевые устройства, через которые проходит сетевой трафик. Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

Первый адрес, который выводит команда **tracert**, — это сетевой шлюз (точка выхода) по умолчанию.

- Сравните вывод команды **tracert** с таблицей адресации, приведенной в начале лабораторной работы. Какой маршрутизатор в данный момент является текущим шлюзом по умолчанию?
-

Шаг 3: Запустите переключение при отказе сетевой инфраструктуры.

- В узле **Metropolis Bank HQ** нажмите коммутатор **HQ_S1**.
- Щелкните вкладку «**Интерфейс командной строки**» (CLI).
- Введите следующие команды, чтобы отключить порт каскадирования Gig0/2:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

Шаг 4: Снова проследите маршрут к внешнему веб-серверу.

- В узле **Metropolis Bank HQ** нажмите ноутбук **Phil**.
 - Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
 - Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.
 - Проследите маршрут к серверу **External Web** в **Интернете**. Для этого в командной строке введите **tracert 209.165.201.10**.
- IP-адреса в выводе команды **tracert** представляют сетевые устройства, через которые проходит сетевой трафик.

Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

-
- e. Первый адрес, который выводит команда **tracert**, — это сетевой шлюз (точка выхода) по умолчанию.

Какой маршрутизатор теперь работает как шлюз по умолчанию?

-
- f. В появившейся **командной строке** введите команду **ipconfig**. Для шлюза по умолчанию показан IP-адрес 10.44.1.1, который не совпадает ни с первым (10.44.1.2), ни со вторым (10.44.1.3) выводом команды **tracert**. Это указывает на то, что маршрутизация трафика шлюза по умолчанию 10.44.1.1 фактически выполняется через резервные маршрутизаторы с различными IP-адресами: R1 с адресом 10.44.1.2 или R2 с адресом 10.44.1.3, если маршрутизатор R1 недоступен.

Учебный вопрос 2: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.

Шаг 1: Откройте командную строку на компьютере Tim's.

- Выберите узел **Gotham Healthcare Branch** и выберите компьютер **Tim**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Проследите маршрут к внешнему веб-серверу.

- Отправьте **ping**-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.
- Для наблюдения за переключением при отказе сетевой инфраструктуры можно использовать команду **constant ping**.

Выполните команду **constant ping** для сервера **External Web**. Для этого в командной строке введите **ping -t 209.165.201.10**.

Сверните окно для компьютера пользователя Tim.

Шаг 3: Запустите переключение при отказе сетевой инфраструктуры.

- В узле **Gotham Healthcare Branch** нажмите коммутатор **S3**.
- Перейдите на вкладку **CLI**.
- Введите следующие команды, чтобы отключить порт каскадирования Gig0/2:

`enable`

`configure terminal`

`interface GigabitEthernet0/2`

`shutdown`

Шаг 4: Снова проследите маршрут к внешнему веб-серверу.

- В узле **Gotham Healthcare Branch** разверните окно, отображающее компьютер пользователя Tim.
- Подождите 30–60 секунд. Также можно наблюдать за индикаторами соединений коммутационного порта в сетевой инфраструктуре Gotham Healthcare Branch.
- Вывод результатов выполнения команды на компьютере пользователя Tim должен быть аналогичен

следующему:

PC>ping -t 209.165.201.10

Pinging 209.165.201.10 with 32 bytes of data:

Reply from 209.165.201.10: bytes=32 time=47ms TTL=126

Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

Reply from 209.165.201.10: bytes=32 time=43ms TTL=126

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Reply from 209.165.201.10: bytes=32 time=41ms TTL=126

Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

- d. Закройте окно.

По какому кабелю передавались данные при получении ответов на ping-запросы до появления сообщения "Request timed out" (Время ожидания запроса истекло)?

По какому кабелю передавались данные при получении ответов на ping-запросы после появления сообщения "Request timed out" (Время ожидания запроса истекло)?

- e. О какой особенности резервирования коммутаторов для переключения при отказе гигабитного Ethernet-порта свидетельствует этот сценарий?

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов	Шаг 2	10	
	Шаг 2	10	
	Шаг 4	10	
	Шаг 4	10	
Вопрос 2. Наблюдение за переключением при отказе	Шаг 4	5	
	Шаг 4	5	

сетевой инфраструктуры с использованием резервных коммутаторов	Шаг 4	10	
Вопросы		60	
Балл Packet Tracer		40	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.
2. Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.
3. Какой маршрутизатор работает как шлюз по умолчанию?
4. По какому кабелю передавались данные при получении ответов на ping-запросы до появления сообщения "Request timed out" (Время ожидания запроса истекло)?
5. По какому кабелю передавались данные при получении ответов на ping-запросы после появления сообщения "Request timed out" (Время ожидания запроса истекло)?
6. О какой особенности резервирования коммутаторов для переключения при отказе гигабитного Ethernet-порта свидетельствует этот сценарий?

Лабораторная работа № 8.

Тема: Защита уровней обеспечения кибербезопасности

Название задания: Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь осуществлять подключение к веб-серверу.
3. Уметь осуществлять предотвращение незашифрованных сеансов HTTP.
4. Приобрести навыки доступа к межсетевому экрану на сервере электронной почты.
5. Приобрести способность формировать процедуры для управления информационной безопасностью.

Учебные вопросы занятия

1. Подключение к веб-серверу.
2. Предотвращение незашифрованных сеансов HTTP.
3. Доступ к межсетевому экрану на сервере электронной почты.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

В этом задании вы получите доступ к пользователю в узле Metropolis и подключитесь по протоколам HTTP и HTTPS к удаленному веб-серверу. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. С помощью клиентского устройства в узле Metropolis вы протестируете подключение к удаленному веб-серверу. Чтобы обеспечить защиту узла Metropolis, вы запретите незашифрованное соединение с внешними веб-сеансами.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Веб-сервер	—	209.165.201.10	255.255.255.0	Интернет

Учебный вопрос 1: Подключение к веб-серверу.

Шаг 1: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

- Выберите узел **Metropolis Bank HQ** и выберите ПК **Sally**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- Введите URL-адрес **http://www.cisco.corp** и нажмите **Go** (Начать).
- Щелкните ссылку **Login Page** (Страница входа).

Почему пользователь должен быть обеспокоен при отправке информации через этот веб-сайт?

Шаг 2: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

- Откройте **веб-обозреватель** на компьютере Sally's.
- Введите URL-адрес **https://www.cisco.corp** и нажмите Go (Начать).
- Щелкните ссылку **Login Page** (Страница входа).

У пользователя меньше поводов для беспокойства при отправке информации через этот веб-сайт. Почему?

- Закройте компьютер пользователя **Sally**.

Учебный вопрос 2: Запрет незашифрованных сеансов HTTP.

Шаг 1: Настройте маршрутизатор HQ_Router.

- Откройте объект **Metropolis Bank HQ** и выберите маршрутизатор **HQ_Router**.
- Нажмите вкладку **CLI** и нажмите **Enter**.
- Для входа в систему маршрутизатора используйте пароль **cisco**.
- Введите команду **enable**, а затем **configure terminal** для доступа к режиму глобальной настройки.

Чтобы предотвратить передачу незашифрованного HTTP-трафика через головной маршрутизатор, сетевые администраторы могут создать и развернуть списки контроля доступа (ACL).

Следующие команды выходят за рамки этого курса. Они используются для демонстрации возможности предотвращения передачи незашифрованного трафика через маршрутизатор HQ_Router.

- В командной строке **HQ_Router(config)#** в режиме глобальной настройки скопируйте и вставьте показанную ниже конфигурацию списка контроля доступа в **HQ_Router**.

```
!  
access-list 101 deny tcp any any eq 80  
access-list 101 permit ip any any  
!  
int gig0/0  
ip access-group 101 in  
!  
end
```

- f. Закройте маршрутизатор **HQ_Router**.

Шаг 2: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

- a. В узле **Metropolis Bank HQ** нажмите ПК пользователя **Sally**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- c. Введите URL-адрес **http://www.cisco.corp** и нажмите **Go** (Начать).

Может ли компьютер пользователя **Sally** получить доступ к веб-серверу HQ Internet по протоколу HTTP?

Шаг 3: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

- a. Откройте **веб-обозреватель** на компьютере Sally's.
- b. Введите URL-адрес **https://www.cisco.corp** и нажмите Go (Начать).

Может ли компьютер пользователя "Sally" получить доступ к веб-серверу HQ Internet по протоколу HTTP?

- c. Закройте компьютер пользователя **Sally**.

Учебный вопрос 3: Доступ к межсетевому экрану на сервере электронной почты.

- a. В узле **Metropolis Bank HQ** нажмите сервер **Email**.
- b. Нажмите вкладку **Desktop** (Рабочий стол) и выберите **Firewall** (Межсетевой экран). Правила межцевого экрана не заданы.

Чтобы предотвратить отправку или получение через сервер электронной почты трафика, не связанного с ней, сетевые администраторы могут создавать правила межцевого экрана непосредственно на сервере. Либо, как показано ранее, можно использовать списки контроля доступа (ACL) на сетевом устройстве, например, маршрутизаторе.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Подключение к веб-серверу	Шаг 1	15	
	Шаг 2	15	
Вопрос 2. Предотвращение незашифрованных сеансов HTTP	Шаг 2	15	
	Шаг 3	15	
Вопросы		60	
Балл Packet Tracer		40	
Общее число баллов		100	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Почему пользователь должен быть обеспокоен при отправке информации через этот веб-сайт?
2. У пользователя меньше поводов для беспокойства при отправке информации через веб-сайт <https://www.cisco.corp>. Почему?
3. Может ли компьютер пользователя **Sally** получить доступ к веб-серверу HQ Internet по протоколу HTTP?
4. Может ли компьютер пользователя "**Sally**" получить доступ к веб-серверу HQ Internet по протоколу HTTP?

Лабораторная работа № 9.

Тема: Специалисты в области кибербезопасности.

Название задания: Отработка комплексных практических навыков

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить навыки, полученные в процессе освоения учебного материала.
2. Приобрести комплексные практические навыки настройки маршрутизатора беспроводной связи, загрузки и выгрузки файлов с использованием протокола FTP, безопасного подключения к удаленному узлу с использованием VPN и обеспечение защиты маршрутизатора Cisco IOS.

Оборудование и материалы

ПК с установленным Packet Tracer.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
HQ_Router	G0/0	10.44.1.1	255.255.255.0	—
	G0/1	209.165.201.2	255.255.255.248	—
VPN-сервер	NIC	209.165.201.19	255.255.255.248	—
HQ_Wireless	LAN	10.44.1.254	255.255.255.0	10.44.1.1
Сервер FTP/Web	NIC	10.44.1.252	255.255.255.0	10.44.1.1
Сервер BackupFiles	NIC	10.44.2.10	255.255.255.0	10.44.2.1

Сценарий

Данное заключительное занятие поможет отработать многие навыки, полученные в процессе освоения учебного материала. Вы выполните настройку маршрутизатора беспроводной связи, загрузку и выгрузку файлов с использованием протокола FTP, безопасное подключение к удаленному узлу с использованием VPN и обеспечите защиту маршрутизатора Cisco IOS.

Реализация

Примечание. У вас есть доступ только к узлу Metropolis HQ. Вы можете получить доступ ко всем серверам и компьютерам на этом узле для выполнения проверки.

Реализуйте следующие требования:

Компьютер пользователя Sally — Metropolis Bank HQ

- Выгрузите файл **secure.txt** на сервер **FTP/Web**, используя протокол FTP:

- Пользователь **sally**, пароль **ftpaccess**
- Файл для загрузки: **secure.txt**
- Используйте IP-адрес сервера **FTP/Web** из таблицы адресации.
- Подключите компьютер пользователя **Sally** к узлу **Gotham Healthcare Branch** по сети VPN «клиент-узел»:
 - Отправьте ping-запрос на сервер VPN, используя IP-адрес из таблицы адресации.
 - Подключите сеть VPN «клиент-узел», используя имя пользователя **sally** и пароль **vpnsally**
 - Используйте группу **VPNGROUP** и ключ **123**
- Используя VPN-соединение, загрузите файл **transactions.txt** с сервера **BackupFiles** по протоколу FTP:
 - Используйте IP-адрес сервера **BackupFiles** из таблицы адресации.
 - Пользователь **sally**, пароль **securesally**
 - Файл для загрузки: **transactions.txt**

Ноутбук пользователя Phil — Metropolis Bank HQ

- Настройте маршрутизатор **HQ_Wireless**.
 - Используйте IP-адрес маршрутизатора **HQ_Wireless** из таблицы адресации.
 - Используйте веб-обозреватель для настройки маршрутизатора **HQ_Wireless** с ноутбука пользователя **Phil**.
 - Пользователь **admin**, пароль **p@ssword**
 - Замените для SSID значение **DefaultWIFI** на **HQwifi**
 - Настройте SSID как видимый (широковещательный) для беспроводных клиентов.
 - Настройте безопасность беспроводной сети **WPA2 Personal**, используя фразу-пароль **cisco321**.
- Обеспечьте защиту маршрутизатора **HQ_Router**.
 - Используйте IP-адрес маршрутизатора **HQ_Router** из таблицы адресации.
 - Используйте командную строку для подключения к **HQ_Router** по протоколу SSH. Имя пользователя **phil**, пароль **securessh**
 - Используйте команду **enable** и пароль **cisco**.
 - Активируйте функцию отказоустойчивой конфигурации Cisco IOS.
 - Настройте для баннера сообщение дня (motd), включающее фразу **Authorized Access Only**

Ноутбук пользователя Gina — Metropolis Bank HQ

- Подключите ноутбук пользователя **Gina** к беспроводной сети.
 - Создайте соединение с SSID **HQwifi**
 - Используйте PSK-ключ **cisco321**
 - Убедитесь, что на ноутбуке используется **DHCP**

Предлагаемый способ подсчета баллов

Балл Packet Tracer: 90 баллов.

Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
ИД-2 ПК-1	Самостоятельное изучение темы № 1	собеседование	3.00	1.00	4.00
ИД-2 ПК-2					
ИД-3 ПК-2					

ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы № 2	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы № 3	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы №4	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы №5	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы №6	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы № 7	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы № 8	собеседование	3.00	1.00	4.00
ИД-2 ПК-1 ИД-2 ПК-2 ИД-3 ПК-2	Самостоятельное изучение темы №9	собеседование	3.00	1.00	4.00
Итого			27.00	9.00	36.00