



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «**Персональная кибербезопасность**»
для студентов направления подготовки
02.03.01 Математика и компьютерные науки
направленность (профиль)
«**Анализ данных и искусственный интеллект**»

СОДЕРЖАНИЕ

Введение.....	
Указания по технике безопасности при выполнении практических занятий.....	
Занятие № 1. Создание кибермира.....	
Занятие № 2. Общение в кибермире	
Занятие № 3. Шифрование файлов и данных	
Занятие № 4. Проверка целостности файлов и данных	
Занятие № 5. WEP/WPA2 PSK/WPA2 RADIUS	
Занятие № 6. Настройка транспортного режима VPN.....	
Занятие № 7. Резервирование маршрутизаторов и коммутаторов	
Занятие № 8. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе	
Занятие № 9. Отработка комплексных практических навыков	
Список литературы	

Введение

Учебная дисциплина «Персональная кибербезопасность» относится к области современных знаний о способах и средствах защиты персональных данных в киберпространстве. В учебной дисциплине изучаются характеристики киберпреступников и тактики, используемые ими, а также изучаются технологии, средства и процедуры, которые специалисты по кибербезопасности используют для борьбы с киберпреступностью.

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;

Учебно-методическое пособие содержит 9 практических занятий, подлежащих выполнению студентами.

Каждое практическое занятие состоит из следующих разделов:

- наименование занятия;
- цели занятия;
- учебные вопросы занятия;
- теоретическая часть;
- оборудование и материалы;
- общие сведения/сценарий
- таблица адресации
- методические пояснения и рекомендации по выполнению практического занятия;
- содержание отчета;
- контрольные вопросы.

Учебно-методическое пособие содержит список литературы, общий для всех практических занятий.

Указания по технике безопасности при выполнении практических занятий

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в отсутствии видимых повреждений на рабочем месте;
- разместить на столе тетради, учебные пособия так, что бы они не мешали работе на компьютере;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или сотрудника лаборатории.

Требования безопасности во время работы

- ЗАПРЕЩАЕТСЯ: присоединять или отсоединять кабели, трогать разъемы, провода и розетки, открывать системный блок, пытаться самостоятельно устранять неисправности в работе оборудования, приносить и запускать компьютерные игры;
- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной работе;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или сотруднику лаборатории;

Требования безопасности по окончании работы

- доложить руководителю занятий или сотруднику лаборатории о завершении работ;
- привести в порядок и сдать рабочее место сотруднику лаборатории, и доложить руководителю занятий о сдаче.

Занятие № 1. 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 PacketTracer

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 под-сети	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.

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

Шаг 2: Создайте для пользователей учетные записи электронной почты.

- Создайте доменное имя **cisco.corp**.
- 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.

- Выберите компьютер с именем **Sally** и перейдите на вкладку **Desktop** (Рабочий стол).
- 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**
- 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.

- Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.
- Перейдите на вкладку **Services** (Службы) и выберите **NTP**.
- 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?

Занятие № 2. 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 под-сети	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.

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

Шаг 2: Отправка электронного сообщения пользователю Sally.

- a. Нажмите кнопку **Compose** (Создать), чтобы создать электронное сообщение.
 - b. 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.**"
 - c. Нажмите кнопку **Send** (Отправить), чтобы отправить электронное сообщение.
- По какому протоколу письмо было отправлено на сервер электронной почты?
-
-

Шаг 3: Проверка почты пользователем Sally.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер с именем **Sally**.
 - b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
 - c. 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.

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

Шаг 2: Удаленное подключение к FTP-серверу.

- a. Откройте объект **Healthcare at Home** и выберите компьютер с именем **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 **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 ping-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?

Занятие № 3.

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.

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

- 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.

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.

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

В какой форме представлены данные?

Шаг 2: Удаленное подключение к FTP-серверу.

- a. 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 **ftpllogin.txt** и нажмите кнопку **OK**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Bob.

- a. Выделите весь текст, содержащийся в файле **ftpllogin.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 Шаге 2 в Части 3.

Шаг 2: Загрузите файл на компьютер пользователя Bob.

- В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
- 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**.
- В командную строку с подсказкой **ftp>** введите команду **quit**.
- 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.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
- В окне приложения Email (Электронная почта) нажмите кнопку **Receive** (Получить).
- 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**.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **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 **clientinfo.txt** и нажмите кнопку **OK**.
- Выделите весь текст, содержащийся в файле **clientinfo.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, 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?

Занятие № 4. 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 HMAS.

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 HMAS.

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.

- a. Откройте объект **GothamHealthcare Branch** и выберите компьютер с именем **Mike**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- c. Введите URL-адрес **http://www.cisco.corp** и нажмите кнопку **Go** (Перейти).
- d. 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.

- a. Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).
- c. 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.

- a. Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- c. Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).
- d. 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.

- a. Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
 - b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
 - c. Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.
 - d. Введите имя пользователя **mike** и пароль **cisco123**.
 - e. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.
 - f. 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)

- g. Загрузив все файлы, введите команду **quit** в командную строку с подсказкой **ftp>**.
- h. 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.

- a. Откройте объект **GothamHealthcare Branch** и выберите компьютер **Mike**.
- 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 **NEclients.txt** и нажмите кнопку **OK**.
- e. Полностью скопируйте содержимое текстового документа.
- f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://www.tools4noobs.com/online_tools/hash/.
- g. 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).

- h. 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.
- i. 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.

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

- 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. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что критически важный файл **income.txt** находится на компьютере пользователя Bob.
- d. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).
- e. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).
- f. Выберите документ **income.txt** и нажмите кнопку **OK**.
- g. Полностью скопируйте содержимое текстового документа.
- h. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт <http://www.freeformatter.com/hmac-generator.html>.

- i. 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.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).
- c. Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).
- d. 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?

Занятие № 5. 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.

- Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.
- 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**.
- Перейдите на вкладку **Wireless**. Измените идентификатор SSID с **DefaultWIFI** на **HQ**.
- Измените значение параметра Standard Channel (Стандартный канал) на **11 — 2.462GHz**.
- Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).
- Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

- Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **WirelessSecurity** (Защита беспроводной сети).
- В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2-Enterprise**.
- Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. Введите следующие параметры сервера RADIUS:
RADIUS SERVER IP (IP-адрес сервера RADIUS): **10.44.1.252**
Shared Secret (Общий секретный ключ): **ciscosecure**
- Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Настройка сервера RADIUS.

- Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.
- Перейдите на вкладку **Services** (Службы) и выберите раздел **AAA**.
- 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**
Server Type (Тип сервера): **Radius**
- Нажмите **Добавить**.
- 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.
- l. Повторите шаги **a–j** на ноутбуке **Phil**, используя аутентификационную информацию, указанную в описании шага 3е.

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?

Занятие № 6. Часть 1

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.

- а. Выберите анализатор трафика **Cyber Criminals Sniffer** и перейдите на вкладку GUI (Графический интерфейс).

- b. Нажмите кнопку **Clear** (Очистить), чтобы удалить все собранные ранее записи с информацией о трафике.
- c. Сверните окно анализатора трафика **Cyber Criminals Sniffer**.

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

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

- a. Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.
- b. В анализаторе трафика выберите сообщения **FTP** и полностью прокрутите содержимое каждого из сообщений.

Какая информация отображается в виде открытого текста?

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

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

- a. 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.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **VPN**.
- c. 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**
- d. 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.

Занятие № 6. Часть 2

НАСТРОЙКА ТУННЕЛЬНОГО 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-туннеля между объектами Metropolis и Gotham
3. Передача зашифрованного FTP-трафика

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это упражнение, вы будете отслеживать передачу незашифрованного FTP-трафика между двумя различными объектами. Затем вы настроите VPN-туннель между двумя объектами и организуете передачу зашифрованного FTP-трафика. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Пользуясь клиентскими устройствами, которые находятся в различных географических регионах, вы будете передавать данные по протоколу FTP безопасным и небезопасным способами.

Таблица адресации

Устройство	Частный IP-адрес	Маска подсети	Сайт
Сервер резервного копирования файлов	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Передача незашифрованного FTP-трафика

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

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

Шаг 2: Установка небезопасного FTP-соединения с резервным FTP-сервером.

- a. Откройте объект **Metropolis Bank HQ** и выберите ноутбук **Phil**.

- b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **Command Prompt** (Командная строка).
- c. С помощью команды **ipconfig** отобразите текущий IP-адрес компьютера **Phil**.
- d. Установите соединение с резервным файловым сервером **File Backup** объекта **Gotham Healthcare Branch**. Для этого введите команду **ftp 10.44.2.254** в командную строку.
- e. Введите имя пользователя **cisco** и пароль **cisco**, чтобы войти на резервный файловый сервер **File Backup**.

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

- a. Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.
- b. В анализаторе трафика выберите сообщения **FTP** и полностью прокрутите содержимое каждого из сообщений.

Какая информация отображается в виде открытого текста?

Учебный вопрос 2: Настройка VPN-туннеля между объектами Metropolis и Gotham

- a. Откройте объект **Metropolis Bank HQ** и выберите маршрутизатор **HQ_Router**.
- b. Скопируйте параметры IPsec VPN для конфигурации соединения между объектами (ниже) и вставьте скопированные параметры в маршрутизатор **HQ_Router**.

```
enable
configure terminal
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key vpnpass address 209.165.201.19
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
  description VPN connection to Branch_Router
  set peer 209.165.201.19
  set transform-set VPN-SET
  match address 110
!
interface GigabitEthernet0/1
  crypto map VPN-MAP
!
```

```
access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
!
end
copy run start
```

- c. На маршрутизаторе **Branch_Router** объекта **Gotham Healthcare Branch** уже создана соответствующая зеркальная конфигурация сети IPsec VPN.

Учебный вопрос 3: Передача зашифрованного FTP-трафика

Шаг 1: Отправка FTP-трафика с компьютера пользователя Sally на резервный файловый сервер File Backup.

- a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally's**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- c. С помощью команды **ipconfig** отобразите текущий IP-адрес компьютера пользователя **Sally**.
- d. Установите соединение с резервным файловым сервером **File Backup** объекта **Gotham Healthcare Branch**. Для этого введите команду **ftp 10.44.2.254** в командную строку. (может потребоваться 2–5 попыток)
- e. Введите имя пользователя **cisco** и пароль **cisco**, чтобы войти на резервный файловый сервер **File Backup**.
- f. С помощью команды **put** выгрузите файл **FTPutload.txt** на резервный файловый сервер **File Backup**.

Шаг 2: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer

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

Имеются ли FTP-сообщения с IP-адреса компьютера **Sally's**? 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 3. Передача зашифрованного FTP-трафика	Шаг 2	30	
Вопросы		50	
Балл Packet Tracer		50	
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 анализаторе трафика в виде открытого текста?
2. Имеются ли FTP-сообщения с IP-адреса компьютера Sally's в окне анализатора трафика? Дайте пояснение.

Занятие № 7. Часть 1

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.

- а. Выберите узел **Metropolis Bank HQ** и выберите ноутбук **Phil**.

- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Проследите маршрут к внешнему веб-серверу.

- a. Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.
- b. Проследите маршрут к серверу **External Web** в **Интернете**. Для этого в командной строке введите **tracert 209.165.201.10**.
- c. 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.

- d. 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.

- a. В узле **Metropolis Bank HQ** нажмите коммутатор **HQ_S1**.
- b. Щелкните вкладку «Интерфейс командной строки» (CLI).
- c. 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.

- a. В узле **Metropolis Bank HQ** нажмите ноутбук **Phil**.
- b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).
- c. Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.
- d. 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.

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

Какой маршрутизатор теперь работает как шлюз по умолчанию?

- ф. 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.

- c. 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	Шаг 2	10	
	Шаг 2	10	

отказе сетевой инфраструктуры с использованием резервных маршрутизаторов	Шаг 4	10	
	Шаг 4	10	
Вопрос 2. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов	Шаг 4	5	
	Шаг 4	5	
	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?

Занятие № 7. Часть 2

РЕЗЕРВИРОВАНИЕ МАРШРУТИЗАТОРОВ И КОММУТАТОРОВ

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь осуществлять активацию функции CiscoIOSResilientConfiguration.
3. Приобрести способность формировать процедуры для управления информационной безопасностью.

Учебные вопросы занятия

1. Повышение надежности конфигурации IOS
2. Активация функции Cisco IOS Resilient Configuration

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

В ходе выполнения этого задания вы повысите надежность конфигурации IOS маршрутизатора в сетевой инфраструктуре Метрополиса. Затем вы включите функцию отказоустойчивости IOS на маршрутизаторе Cisco. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Для развертывания отказоустойчивой конфигурации IOS будут использоваться клиентские устройства в сетевой инфраструктуре Метрополиса.

Таблица адресации

Устройство	IP-адрес	Маска под-сети	Шлюз по умолчанию	Сайт
HQ_Router	10.44.1.1	255.255.255.0	—	Metropolis Bank HQ

Учебный вопрос 1: Повышение надежности конфигурации IOS

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

- а. Выберите узел **Metropolis Bank HQ** и выберите компьютер пользователя **Sally**.
- б. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Выполните удаленное подключение к маршрутизатору HQ_Router.

- а. Установите с маршрутизатором **HQ_Router** соединение по протоколу SSH. Для этого в командной строке введите **ssh -l admin 10.44.1.1**. В открывшемся окне введите пароль **cisco12345**.
- б. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.

В командной строке должно отображаться следующее:

HQ_Router#

- с. Было ли показано предупреждающее сообщение, препятствующее доступу неавторизованных пользователей к маршрутизатору HQ_Router?
-
-

Шаг 3: Создайте правовое уведомление на маршрутизаторе HQ_Router.

- а. В командной строке HQ_Router# введите команду **configure terminal** для перехода в режим глобальной настройки.
- б. В командной строке HQ_Router(config)# вставьте следующие команды:
- ```
banner motd #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
Для доступа к этому устройству или его настройкам необходимо явное разрешение.
Несанкционированные попытки и действия, предпринятые с целью доступа к этой системе или ее использования, могут вести к гражданско-правовой и/или уголовной ответственности.
Все действия, выполняемые на этом устройстве, регистрируются и отслеживаются.
#
```
- с. В командной строке HQ\_Router(config)# введите команды **end** и **logout** для завершения соединения с маршрутизатором **HQ\_Router**.
- д. Снова установите соединение по протоколу SSH с маршрутизатором **HQ\_Router** с компьютера пользователя **Sally**. Пароль SSH — **cisco12345**.
- Был ли показан какой-либо дополнительный текст или информационное сообщение при успешном подключении к **HQ\_Router**? Что было показано?
- 
- 
- 

**Шаг 4: Включите защиту паролем на маршрутизаторе HQ\_Router.**

- а. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.
- б. Войдите в режим глобальной конфигурации с помощью команды **configure terminal**. В командной строке HQ\_Router(config)# вставьте следующие команды:
- ```
!шифрует незашифрованные пароли в running-config  
service password-encryption
```
- !все новые сконфигурированные пароли должны содержать не менее 10 символов
- ```
security passwords min-length 10
```

**Учебный вопрос 2: Активация функции Cisco IOS Resilient Configuration**

**Шаг 1: Просмотрите текущий образ IOS.**

- а. После подключения по протоколу SSH с компьютера **Sally** введите команду **exit** для возврата к командной строке HQ\_Router#.

- b. Введите команду **dir flash:** для просмотра текущего файла IOS.bin.  
Как называется текущий файл .bin в команде flash?
- 
- 

## Шаг 2: Обеспечьте защиту текущего образа и конфигурации.

- a. В командной строке HQ\_Router# введите команду **configure terminal** для перехода в режим глобальной настройки.
- b. С помощью команды **secure boot-image** в командной строке HQ\_Router(config)# активируйте резервное копирование образа IOS и запретите показ файла IOS в выводе каталога, а также удаление защищенного файла IOS.
- c. Используйте команду **secure boot-config** в командной строке HQ\_Router(config)#, чтобы сохранить защищенную копию текущей конфигурации и предотвратить удаление защищенного файла конфигурации.
- d. Вернитесь в привилегированный режим EXEC с помощью команды **exit**. Введите команду **dir flash:** для просмотра текущего файла IOS.bin.

Показан ли в выводе файл IOS.bin? \_\_\_\_\_

- e. В командной строке HQ\_Router# введите команду **show secure bootset** для просмотра статуса образа Cisco IOS и резервного копирования конфигурации.

### Предлагаемый способ подсчета баллов

| Вопросы занятия                                               | Шаги вопроса | Максимальное количество баллов | Заработанные баллы |
|---------------------------------------------------------------|--------------|--------------------------------|--------------------|
| Вопрос 1. Повышение надежности конфигурации IOS               | Шаг 2        | 10                             |                    |
|                                                               | Шаг 3        | 10                             |                    |
| Вопрос 2. Активация функции Cisco IOS Resilient Configuration | Шаг 1        | 10                             |                    |
|                                                               | Шаг 2        | 10                             |                    |
| <b>Вопросы</b>                                                |              | <b>40</b>                      |                    |
| <b>Балл Packet Tracer</b>                                     |              | <b>60</b>                      |                    |
| <b>Общее число баллов</b>                                     |              | <b>100</b>                     |                    |

### 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. Было ли показано предупреждающее сообщение, препятствующее доступу неавторизованных пользователей к маршрутизатору **HQ\_Router**?
2. Был ли показан какой-либо дополнительный текст или информационное сообщение при успешном подключении к **HQ\_Router**? Что было показано?
3. Как называется текущий файл .bin в команде flash?
4. Показан ли в выводе файл IOS.bin?

## Занятие № 8.

### 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 под-сети | 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.

- a. Выберите узел **Metropolis Bank HQ** и выберите ПК **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).
- d. 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.**

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

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

---

- d. Закройте компьютер пользователя **Sally**.

**Учебный вопрос 2: Запрет незашифрованных сеансов HTTP.**

**Шаг 1: Настройте маршрутизатор HQ\_Router.**

- a. Откройте объект **Metropolis Bank HQ** и выберите маршрутизатор **HQ\_Router**.
- b. Нажмите вкладку **CLI** и нажмите **Enter**.
- c. Для входа в систему маршрутизатора используйте пароль **cisco**.
- d. 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.

- e. 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 меж сетевого экрана не заданы.

Чтобы предотвратить отправку или получение через сервер электронной почты трафика, не связанного с ней, сетевые администраторы могут создавать правила меж сетевого 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                             |                    |
| <b>Вопросы</b>                                        |              | <b>60</b>                      |                    |
| <b>Балл Packet Tracer</b>                             |              | <b>40</b>                      |                    |
| <b>Общее число баллов</b>                             |              | <b>100</b>                     |                    |

### **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.com>. 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?

## Занятие № 9. 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 выгрузки: **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.

### Список литературы

1. Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах "Информ-2016": Сборник научных трудов II Международной научно-технической конференции 26-27 мая 2016 г. / ред. кол. В. М. Довгаль, Ю. Н. Быков, Л. С. Крыжевич ; Курск. гос. ун-т, Нац. ун-т Трухильо (Перу), Евраз. нац. ун-т, ВГТУ, РГРУ, ТГУ, БелГТУ, Ч. 1. - Курск : Курск. гос. ун-т, 2016.
2. Алгулиев, Р. М. Киберфизические системы: основные понятия и вопросы обеспечения безопасности / Р. М. Алгулиев, Я. Н. Имамвердиев, Л. В. Сухостат [Текст] // Информационные технологии. – 2017.
3. Емельянова, Н. З. Защита информации в персональном компьютере : [учеб. пособие] / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М. : ФОРУМ, 2009. - 368 с.
4. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 6-е изд., стер. – Москва : Академия, 2012. – 336 с.
5. Козлов, В. Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М.: Горячая линия-ТЕЛЕКОМ, 2002. – 336 с.
6. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс / А.Н. Андрончик. - Екатеринбург: Издательство Уральского университета, 2014. - 179 с. - ISBN 978-5-7996-1201-6

## **МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

по организации и проведению самостоятельной работы  
по дисциплине **«Персональная кибербезопасность»**  
для студентов направления подготовки  
**02.03.01 «Математика и компьютерные науки»**  
направленность (профиль)  
**«Анализ данных и искусственный интеллект»**

## Введение

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;

В результате освоения дисциплины обучающийся должен:

| Перечень компонентов                                                                                                                                                                                                                                                                                | Технологии формирования компетенции          | Средства и технологии оценки    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------|
| <b>Знать:</b> этические ценности специалиста по обеспечению кибербезопасности<br>архитектуру управления безопасностью ИТ-среды<br>уровни обеспечения кибербезопасности<br>средства противодействия угрозам кибербезопасности                                                                        | лекции, самостоятельная работа               | тестирование, письменный отчет  |
| <b>Уметь:</b> применять заповеди компьютерной этики для решения задач межличностного и межкультурного взаимодействия<br>определять угрозы персональной кибербезопасности, уязвимости и атаки<br>применять способы физической защиты сетевых устройств<br>реагировать на инциденты кибербезопасности | практические занятия, самостоятельная работа | собеседование, письменный отчет |
| <b>Владеть:</b> навыками использования инструментов персональной кибербезопасности<br>технологиями противодействия угрозам персональной кибербезопасности<br>способами защиты данных<br>технологиями и процедурами для защиты систем, устройств и данных, составляющих сетевую инфраструктуру       | практические занятия, самостоятельная работа | собеседование, письменный отчет |

## **Общая характеристика самостоятельной работы студента**

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области документоведения.

На практических занятиях формируются умения, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим занятиям, завести новую тетрадь для конспектирования лекций и выполнения практических работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное выполнение заданий по заданным темам;
- самостоятельное изучение учебного материала по заданным темам;
- подготовка к практическим заданиям, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

- 1) для овладения знаниями:
  - чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
  - работа с нормативными документами;
  - поиск информации в Интернет;
- 2) для закрепления и систематизации знаний:
  - работа с конспектом лекции (обработка текста);
  - повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
  - составление плана и тезисов ответа или графическое изображение структуры ответа;
  - составление таблиц для систематизации учебного материала;
  - изучение нормативных документов;
  - ответы на контрольные вопросы;
- 3) для формирования умений:

- подготовка к практическим занятиям;
- решение задач и практических заданий;
- подготовка отчетов по практическим занятиям;
- рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим занятиям, а также варианты тестовых заданий.

#### Технологическая карта самостоятельной работы студента

| Код реализуемой компетенции | Вид деятельности студентов                                                                                                     | Итоговый продукт самостоятельной работы | Средства и технологии оценки | Объем акад. часов |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------------------------|-------------------|
| ПК-3                        | Самостоятельное изучение темы.<br>Подготовка к практическим занятиям.<br>Самостоятельное выполнение заданий по заданным темам. | Конспект. Письменный отчет              | Собеседование                | 36                |
| <b>Итого за семестр</b>     |                                                                                                                                |                                         |                              | 36                |
| <b>Итого</b>                |                                                                                                                                |                                         |                              | <b>36</b>         |

#### Самостоятельное изучение тем лекций

| № п/п | Темы для самостоятельного изучения                        | Рекомендуемые источники информации (№ источника) |                |              |                  |
|-------|-----------------------------------------------------------|--------------------------------------------------|----------------|--------------|------------------|
|       |                                                           | Основная                                         | Дополнительная | Методическая | Интернет-ресурсы |
| 1     | Тема: Кибербезопасность: мир специалистов и преступников. | 1                                                | 1-5            | 1            | 1-4              |
| 2     | Тема: Куб кибербезопасности.                              | 1                                                | 1-5            | 1            | 4                |
| 3     | Тема: Свойства противодействия угрозам кибербезопасности. | 1                                                | 1-5            | 1            | 4                |
| 4     | Тема: Угрозы кибербезопасности, уязвимости и атаки.       | 1                                                | 1-5            | 1            | 4                |
| 5     | Тема: Способы защиты информации ограниченного доступа.    | 1                                                | 1-5            | 1            | 4                |
| 6     | Тема: Способы обеспечения целостности данных.             | 1                                                | 1-5            | 1            | 4                |
| 7     | Тема: Концепция «пять девяток».                           | 1                                                | 1-5            | 1            | 4                |
| 8     | Тема: Защита уровней обеспечения кибербезопасности.       | 1                                                | 1-5            | 1            | 4                |
| 9     | Тема: Специалисты в области кибербезопасности.            | 1                                                | 1-5            | 1            | 4                |



## ЗАДАНИЯ ПО ТЕМАМ УЧЕБНОЙ ДИСЦИПЛИНЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

### Задания по теме «Кибербезопасность: мир специалистов и преступников»

#### Задание 1. Идентификация угроз

##### Задачи

Изучение возможностей обеспечения безопасности, с помощью которых организации защищают данные.

**Часть 1. Изучение угрозы, исходящей от кибератак**

**Часть 2. Триада КИД**

##### Общие сведения/сценарий

Угрозы, существующие в современном кибермире, представляют реальную опасность и вполне могли бы перевернуть нынешний компьютеризированный мир с ног на голову. Об этих угрозах должен знать каждый, однако полностью нейтрализовать их смогут только профессионалы, способные вовремя распознать опасность и переиграть киберпреступников. Силами CompTIA, Cisco Systems, ISC2 и других организаций созданы и реализуются программы по обучению и сертификации специалистов в сфере кибербезопасности.

##### Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

##### Изучение угрозы, исходящей от кибератак

Кибератаки возглавляют рейтинг угроз, представляющих опасность для государств всего мира. В сознании общества угроза национальной или мировой безопасности чаще всего ассоциируется с физическим нападением или оружием массового поражения. В действительности же наибольшую угрозу для двадцати с лишним государств представляют именно кибератаки. Выход кибератак на передний план отражает соответствующие изменения в обществе. Мы учимся, делаем покупки, общаемся, путешествуем и живем, постоянно взаимодействуя с компьютерами и компьютерными сетями. Компьютерные системы контролируют почти все аспекты жизни современного человека. Поэтому нарушение работы компьютерных систем и сетевых инфраструктур может иметь катастрофические последствия. В частности, кибератаки могут быть направлены на системы выработки и распределения электроэнергии, системы очистки и подачи воды, транспортные и финансовые системы. Системы всех перечисленных выше категорий неоднократно становились мишенями кибератак. Просмотрите представленный ниже видеоролик. Объединитесь в группы по 3–4 человека. Просмотрев видеоролик, ответьте на следующие вопросы.

##### Исследование угроз.

Шаг 1 посвящен исследованию угроз.

- а. Нажмите [здесь \(https://www.youtube.com/watch?v=WnUuLzXCIEk\)](https://www.youtube.com/watch?v=WnUuLzXCIEk), чтобы просмотреть видеоролик. Какое оружие является самым опасным, по мнению авторов видеоролика? Почему? Согласны ли вы с этим мнением?

- 
- 
- 
- б. Перечислите пять способов нарушения закона с помощью компьютеров. Могут ли последствия перечисленных вами преступлений затронуть лично вас? Приходилось ли вам или вашим близким иметь дело с последствиями таких преступлений?
- 
- 
- 

- с. Совершались ли реальные преступления, связанные с угрозами, которые описаны в видеоролике? Нажмите [здесь](http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=1) ([http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?\\_r=1](http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=1)), чтобы больше узнать об этих атаках.
- 
- 
- 

#### **Изучение недавних атак.**

- а. Последствия и масштаб недавних кибератак обеспокоили многих руководителей в частных и государственных структурах. Нажмите [здесь](http://www.information-age.com/technology/security/123460657/top-10-most-devastating-cyber-hacks-2015) (<http://www.information-age.com/technology/security/123460657/top-10-most-devastating-cyber-hacks-2015>), чтобы прочесть о десяти наиболее разрушительных кибератаках 2015 г.  
Сколько людей затронула утечка данных в Управлении кадровой службы США?
- 
- 
- 

- б. Опишите атаку TalkTalk, предпринятую в 2015 г. Кто совершил атаку? Что украли киберпреступники?
- 
- 
- 

#### **Конфиденциальность, целостность и доступность**

В основе кибербезопасности лежат три основополагающих принципа — конфиденциальность, целостность и доступность. Эти принципы образуют триаду КЦД и являются важнейшими элементами кибербезопасности. Каждый специалист по кибербезопасности должен хорошо понимать эти принципы.

## Изучение триады КЦД

- а. Нажмите [здесь \(https://www.youtube.com/watch?v=bhLbnOa4wno\)](https://www.youtube.com/watch?v=bhLbnOa4wno), чтобы просмотреть видеоролик. Что понимается под конфиденциальностью данных? Почему конфиденциальность данных, принадлежащих людям и организациям, имеет большое значение?

---

---

---

- б. Что понимается под целостностью данных? Назовите три способа нарушения целостности или достоверности данных.

---

---

---

- с. Что понимается под доступностью систем? Что может произойти в случае недоступности критически важной компьютерной системы?

---

---

---

## Изучение кибератак.

Нажмите [здесь \(https://www.youtube.com/watch?v=CMsp8WiBxzM&index=85&list=PL6FEA443253B44EC2\)](https://www.youtube.com/watch?v=CMsp8WiBxzM&index=85&list=PL6FEA443253B44EC2), чтобы просмотреть видеоролик. Чего пытались добиться киберпреступники? В какое время суток была совершена атака? Верно ли, что сетевые атаки чаще совершаются в нерабочее время? Почему?

---

---

---

## Задание 2. Задачи профессионалов в сфере кибербезопасности

### Задачи

Изучение возможностей обеспечения безопасности, применяемых для защиты данных в таких компаниях, как Google и Cisco.

#### Часть 1. Защита ваших данных

#### Часть 2. Усиление безопасности вашей учетной записи Google

### Общие сведения/сценарий

Эта глава знакомит студента с кибермиром. В кибермире присутствует огромное количество хранилищ, которые обрабатывают немыслимое количество данных, принад-

лежащих людям и организациям. Специалисты по кибербезопасности должны быть хорошо знакомы со всеми видами защитных механизмов, которые необходимо применять в организациях для обеспечения безопасности хранимых и обрабатываемых данных. В ходе выполнения этого задания вы ближе познакомитесь с компанией Google, которая относится к числу мировых лидеров по объему обрабатываемых данных. Вы просмотрите два видеоролика и ответите на ряд вопросов. Каждый из видеороликов посвящен отдельному аспекту кибербезопасности в Google. Выполнив это задание, вы приобретете новые знания о мерах и сервисах обеспечения безопасности, применяемых в таких организациях, как Google, для защиты информации и информационных систем.

### **Видеоролики:**

[Как в Google защищают ваши данные \(https://www.youtube.com/watch?v=TQoKFovvigI\)](https://www.youtube.com/watch?v=TQoKFovvigI)

[Ключ безопасности \(https://www.youtube.com/watch?v=LUHOs\\_ggvi4\)](https://www.youtube.com/watch?v=LUHOs_ggvi4)

### **Необходимые ресурсы**

ПК или мобильное устройство с доступом к Интернету

### **Защита ваших данных**

Компания Google является одним из лидеров по объему хранимых персональных данных. На Google приходится около 50 % всех операций поиска в Интернет. Кроме того, Google владеет сервисом YouTube, операционной системой Android и множеством других платформ, с которых поступает огромное количество собираемых данных. Выполняя это упражнение, вы просмотрите короткий видеоролик и попытаетесь определить ряд защитных мер, применяемых специалистами Google по кибербезопасности для защиты ваших данных.

### **Откройте браузер и просмотрите следующий видеоролик:**

[Как в Google защищают ваши данные \(https://www.youtube.com/watch?v=TQoKFovvigI\)](https://www.youtube.com/watch?v=TQoKFovvigI)

- a. Как в Google гарантируют отсутствие вредоносного ПО на серверах, которые устанавливаются в центрах обработки данных? Ведь серверы могут быть заражены уже в процессе производства.

---

---

---

- b. Как контролируют физический доступ к серверам в центрах обработки данных Google?

---

---

---

- c. Как в Google защищают данные, находящиеся на серверах?

---

---

---

---

### Выявление уязвимостей, связанных с данными.

- с. Из содержания видеоролика следует, что данные, хранящиеся в центрах обработки данных Google, хорошо защищены, однако не все данные, используемые в процессе вашего взаимодействия с Google, находятся в центрах обработки данных Google. Куда еще попадают ваши данные при работе с поисковой системой Google?

- д. Можно ли защитить данные при работе с поисковой системой Google? Какие меры можно принять для защиты ваших данных?

---

---

### Усиление безопасности вашей учетной записи Google

Важнейшей задачей при работе с веб-сервисами, включая сервисы Google, является защита идентификационных данных учетной записи (имя пользователя и пароль). Ситуация осложняется тем, что одна и та же учетная запись зачастую используется для аутентификации на нескольких веб-сайтах, например на веб-сайтах Facebook, Amazon и LinkedIn. Существует несколько способов усиления защиты данных вашей учетной записи Google. Можно включить двухэтапную аутентификацию (после успешного ввода имени пользователя и пароля нужно будет вводить одноразовый код доступа). Кроме того, Google поддерживает аутентификацию с помощью ключей безопасности. Выполняя это упражнение, вы просмотрите короткий видеоролик и попытаетесь определить меры, которые можно принять для защиты данных вашей учетной записи при работе с интернет-сервисами.

### Откройте браузер и просмотрите следующий видеоролик:

**Ваш ключ: проще, быстрее и безопаснее**  
**([https://www.youtube.com/watch?v=LUHOs\\_ggvi4](https://www.youtube.com/watch?v=LUHOs_ggvi4))**

- а. Что понимается под двухэтапной аутентификацией? Каким образом такая аутентификация защищает вашу учетную запись Google?

- б. Что собой представляет ключ безопасности и какую функцию он выполняет? Можно ли использовать ключ безопасности в нескольких системах?

- 
- 
- с. Нажмите [здесь \(https://support.google.com/accounts/answer/6103543?hl=en\)](https://support.google.com/accounts/answer/6103543?hl=en), чтобы открыть страницу с ответами на часто задаваемые вопросы о ключе безопасности. Если в учетной записи настроена аутентификация с помощью ключа безопасности, можно ли войти в эту учетную запись, не имея ключа безопасности?
- 
- 
- 

### **Исключение несанкционированного доступа к учетной записи Gmail.**

Почта Gmail пользуется большой популярностью. В Google зарегистрировано более миллиарда активных учетных записей Gmail. В Gmail предусмотрена удобная функция, позволяющая предоставить другим пользователям доступ к вашей учетной записи. При организации такого доступа создается совместная учетная запись электронной почты. С помощью этой функции хакеры могут получить несанкционированный доступ к вашей учетной записи Gmail. Проверьте вашу учетную запись. Для этого войдите в свою учетную запись Gmail и нажмите на шестеренку, которая находится в правом верхнем углу (Настройки). На странице «Настройки» отображается строка с названиями разделов (сразу под заголовком «Настройки») — «Общие», «Ярлыки», «Папка "Входящие"», «Аккаунты и импорт», «Фильтры и заблокированные адреса» и т. д.

Выберите раздел **Учетные записи и импорт**. Проверьте пункт **Предоставить доступ к своей учетной записи**. Удалите всех неавторизованных пользователей, имеющих доступ к вашей учетной записи.

### **Проверка активности учетной записи Gmail.**

В Gmail можно просмотреть журнал активности учетной записи пользователя, чтобы убедиться в том, что доступ к учетной записи имеет только ее владелец. С помощью этой функции можно определить, какие пользователи получали доступ к учетной записи и где находился каждый из пользователей в момент получения доступа. Проверьте, входил ли в учетную запись кто-либо кроме вас. Для этого воспользуйтесь функцией **Последние действия в учетной записи**. Чтобы воспользоваться функцией **Последние действия в учетной записи**, выполните следующие действия.

Войдите в свою учетную запись Gmail.

Обратите внимание на строку **Последние действия в учетной записи**: внизу страницы. С помощью ссылки, которая находится под этой строкой, можно обнаружить неавторизованных пользователей, получавших доступ к учетной записи, и определить местоположение этих пользователей.

Непосредственно под этой строкой находится гиперссылка «Дополнительная информация». Перейдите по гиперссылке «Дополнительная информация».

Просмотрите журнал активности учетной записи. Чтобы отключить неавторизованных пользователей (если таковые найдутся) от вашей учетной записи, нажмите кнопку **Выйти из всех остальных веб-сеансов**. После этого необходимо сменить пароль,

иначе неавторизованные пользователи смогут восстановить доступ к вашей учетной записи.

### Задание по теме «Куб кибербезопасности»

#### Задание 3. Игра «Подбор» по теме «Волшебный куб кибербезопасности» на веб-сайте Quizlet

##### Задачи

Изучение трех измерений волшебного куба кибербезопасности и элементов этих измерений.

##### Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

##### Общие сведения/сценарий

Куб Маккамбера, разработанный Джоном Маккамбером в 1992 г., применяется в качестве архитектуры или модели при разработке и оценке мер обеспечения безопасности применительно к информации и информационным системам. Согласно этой архитектуре, специалист по кибербезопасности должен рассматривать информационные ресурсы, ориентируясь на три основополагающих принципа кибербезопасности — конфиденциальность, целостность и доступность. Модель строится на трех измерениях, каждое из которых содержит три элемента.

##### Первое измерение. Принципы кибербезопасности: КИЦД

**Конфиденциальность.** Исключить намеренное или случайное раскрытие конфиденциальной информации.

**Целостность.** Исключить намеренное или случайное изменение информации, в результате которого может быть нарушена ее надежность.

**Доступность.** Обеспечить надежный и своевременный доступ авторизованных лиц к информации и информационным системам.

##### Второе измерение. Состояния информации (данных)

**Хранение.** Данные в состоянии покоя (хранятся в памяти или на флеш-диске).

**Передача.** Передача данных между различными системами.

**Обработка.** Выполнение операций над данными (изменение, резервное копирование, корректирование и др.).

##### Третье измерение. Механизмы и контрмеры безопасности

**Политика и практические методы.** Административный контроль (политика информационной безопасности, процедуры, указания, руководящие директивы и др.).

**Человеческие факторы.** Каждый пользователь информационной системы должен понимать свою роль и ответственность. Необходимы соответствующие образовательные программы.

**Технологии.** Программные и аппаратные решения, предназначенные для защиты информационных систем (антивирусы, межсетевые экраны, системы обнаружения/предотвращения вторжений и др.).

##### Обзор веб-сайта Quizlet

Перейдите на веб-сайт [Quizlet \(https://quizlet.com/135368588/cybersecurity-essentials-flash-cards/\)](https://quizlet.com/135368588/cybersecurity-essentials-flash-cards/) и просмотрите материал «Основы кибербезопасности —

**волшебный куб кибербезопасности». Для просмотра не обязательно иметь учетную запись на этом веб-сайте.**

Просмотрите список терминов и определений.

Нажмите значок «Карточки». Проверьте свои знания, пройдя все десять карточек.

Выберите в меню пункт «Подбор». Прочтите сообщение и нажмите соответствующую кнопку, чтобы начать игру.

Перенесите каждый термин к соответствующему определению.

## **Задание по теме «Свойства противодействия угрозам кибербезопасности»**

### **Задание 4. Установка виртуальной машины на ПК**

#### **Задачи**

**Часть 1. Подготовка компьютера для виртуализации**

**Часть 2. Импорт виртуальной машины в реестр устройств приложения VirtualBox**

#### **Общие сведения/сценарий**

За последние 10 лет вычислительная мощность компьютеров увеличилась в разы, а разнообразие вычислительных ресурсов поражает. Большой объем оперативной памяти и многоядерные процессоры позволяют эффективно использовать виртуализацию. При виртуализации один или несколько виртуальных компьютеров работают на одном физическом компьютере. Виртуальные компьютеры, работающие на базе физического компьютера, называются виртуальными машинами. Часто виртуальную машину называют гостевой системой, а физический компьютер — хостом. Любой пользователь современного компьютера с современной ОС может работать с виртуальными машинами.

Мы подготовили файл образа виртуальной машины для установки на вашем компьютере. В ходе выполнения этого задания вы загрузите этот файл образа и затем импортируете его с помощью приложения для виртуализации настольных систем, например, VirtualBox.

#### **Необходимые ресурсы**

Компьютер с ОЗУ не менее 2 ГБ и 8 ГБ свободного дискового пространства  
Высокоскоростной доступ в Интернет для загрузки приложения Oracle VirtualBox и файла образа виртуальной машины.

**Примечание.** Размер файла образа составляет около 2,5 Гбайт. За время работы с виртуальной машиной объем файла может увеличиться до 5 Гбайт. После импорта виртуальной машины файл образа можно удалить. В случае если файл образа предполагается сохранить, понадобится не менее 8 Гбайт свободного дискового пространства.

**Примечание.** Установка и запуск 64-разрядных виртуальных машин на физическом хостовом компьютере возможны только в 64-разрядной системе, при этом в BIOS должна быть включена технология аппаратной виртуализации. Если образ виртуальной машины установить не удастся, попробуйте перезагрузить компьютер, войти в меню настройки BIOS и включить аппаратную виртуализацию в разделе расширенной настройки системы.

#### **Подготовка хост-компьютера к виртуализации**

Выполняя часть 1, вы загрузите и установите программное обеспечение для виртуализации настольных систем, а также загрузите файл образа для выполнения заданий этого курса. В ходе этого задания вы будете пользоваться виртуальной машиной с операционной системой Linux.

## Загрузка и установка VirtualBox

Для работы с файлом образа можно загрузить и установить один из двух программных продуктов для виртуализации — VMware Workstation Player или Oracle VirtualBox. В этом задании вы будете пользоваться программным обеспечением VirtualBox.

Перейдите на веб-страницу <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>.

Выберите файл установки в соответствии с установленной операционной системой и загрузите его.

Загрузив файл для установки VirtualBox, запустите установщик и выполните установку с параметрами по умолчанию.

## Загрузка файла образа виртуальной машины

Файл образа имеет формат OVF (Open Virtualization Format). OVF — открытый стандарт для «упаковки» и распространения виртуальных устройств. Пакет OVF содержит несколько файлов, которые помещаются в общий каталог. Этот каталог распространяется в виде пакета OVA. Пакет OVA содержат все файлы OVF, необходимые для развертывания виртуальной машины. Виртуальная машина, созданная для этого задания, экспортирована согласно стандарту OVF.

Нажмите [здесь \(https://static-course-assets.s3.amazonaws.com/CyberEss/files/Ubuntu\\_CyberEss.ova\)](https://static-course-assets.s3.amazonaws.com/CyberEss/files/Ubuntu_CyberEss.ova), чтобы загрузить файл образа виртуальной машины.

**Примечание.** Объем файла составляет 2,5 Гбайт. Загрузка файла может продолжаться более часа. Фактическая скорость загрузки зависит от пропускной способности вашего интернет-подключения.

## Импорт виртуальной машины в реестр устройств приложения VirtualBox

Выполняя часть 2, вы импортируете виртуальную машину в приложение VirtualBox и запустите ее.

## Импорт виртуальной машины в VirtualBox

Откройте **VirtualBox**. Выберите в меню пункты **Файл>Импорт устройств...**, чтобы импортировать образ виртуальной машины.

Откроется новое окно. Укажите местоположение файла .OVA.

После этого появится окно с параметрами импортируемой машины. Установите флажок **Сгенерировать новые MAC-адреса для всех сетевых адаптеров**, расположенный в нижней части окна. Остальные параметры менять не следует. Нажмите **Импорт**.

По завершении процесса импорта вы увидите новую виртуальную машину в списке виртуальных машин VirtualBox (левая панель). Теперь виртуальная машина готова к работе.

## Запуск виртуальной машины и вход в операционную систему

В реестре устройств слева выберите виртуальную машину, с которой будете работать.

Нажмите кнопку **Запустить**. На этой кнопке изображена зеленая стрелка (находится в верхней части окна приложения VirtualBox). Появится новое окно, в котором начнется процесс загрузки виртуальной машины.

**Примечание.** Если виртуальная машина не запускается, следует отключить контроллер USB (для этого откройте окно настройки виртуальной машины и в разделе "USB" снимите флажок «Включить контроллер USB») или загрузить и установить пакет Oracle VM VirtualBox Extension Pack с веб-страницы загрузки программного обеспечения VirtualBox.

По завершении процесса загрузки виртуальная машина запросит имя пользователя и пароль. Выполните вход на виртуальную машину, используя следующие учетные данные.

**Имя пользователя:** cisco

**Пароль:** password

Выполнив вход, вы увидите рабочий стол, панель запуска приложений (внизу), значки на рабочем столе, а также меню приложений (вверху).

**Примечание.** Окно, в котором работает виртуальная машина, следует рассматривать как отдельный компьютер, не имеющий связи с хостом (то есть компьютером, внутри которого запущена виртуальная машина). Например, без установки специальных программных средств вы не сможете копировать и вставлять содержимое через буфер обмена из гостевой операционной системы в хостовую и наоборот. Обратите внимание на фокус клавиатуры и мыши. После нажатия клавиши в окне виртуальной машины ввод с мыши и клавиатуры направляется в гостевую операционную систему. При этом хостовая операционная система не регистрирует нажатия клавиш и перемещение мыши. Чтобы вернуть фокус клавиатуры и мыши в хостовую операционную систему, нажмите правую клавишу **CTRL**.

### Начало работы с виртуальной машиной

Виртуальная машина Ubuntu\_CyberEss, которую вы только что установили, предназначена для выполнения заданий в операционной системе Ubuntu. Изучите следующие значки.

Значки запуска приложений расположены на панели слева (перечислены сверху вниз).

Поиск

Файловый менеджер

Веб-браузер Firefox

LibreOffice Writer, LibreOffice Calc, LibreOffice Impress

Центр приложений Ubuntu

Amazon

Установка системы

Терминал

Корзина

Откройте приложение терминала. Введите команду **ip address** в командную строку, чтобы определить IP-адрес виртуальной машины.

Какой IP-адрес назначен виртуальной машине?

---

Найдите и запустите веб-браузер. Можете ли вы перейти на страницу поисковой системы, которой вы обычно пользуетесь? \_\_\_\_\_

Нажмите правую клавишу Ctrl, чтобы отменить захват ввода виртуальной машиной.  
Теперь в меню, которое находится в верхней части окна виртуальной машины, выберите пункты **Файл>Заккрыть...**, чтобы закрыть виртуальную машину. Какие параметры доступны?

---

---

---

Нажмите селективную кнопку **Сохранить состояние машины** и кнопку **ОК**.  
При следующем запуске виртуальной машины будет восстановлено текущее состояние операционной системы.

### Вопросы для обсуждения

Назовите преимущества и недостатки виртуальных машин.

---

---

---

---

---

---

## Задания по теме «Угрозы кибербезопасности, уязвимости и атаки»

### Задание 5. Аутентификация, авторизация и учет

#### Задачи

Выбор соответствующих методов аутентификации, авторизации или разграничения доступа для заданного сценария

Использование лучших практик установки и настройки средств контроля безопасности при управлении учетными записями

**Часть 1. Создание групп, пользователей и паролей в операционной системе Linux**

**Часть 2. Проверка пользователей, групп и паролей**

**Часть 3. Использование символьного обозначения разрешений**

**Часть 4. Абсолютное обозначение разрешений**

#### Общие сведения/сценарий

Вы будете применять меры обеспечения безопасности на хостовой машине, выполняя следующие операции.

Создание групп, пользователей и паролей

Проверка групп, пользователей и паролей

Назначение разрешений с использованием символьного обозначения

Назначение разрешений с использованием абсолютного обозначения

#### Необходимые ресурсы

Компьютер с операционной системой Ubuntu 16.04 LTS, которая установлена в виртуальной машине VirtualBox или VMware.

#### Создание групп, пользователей и паролей в операционной системе Linux

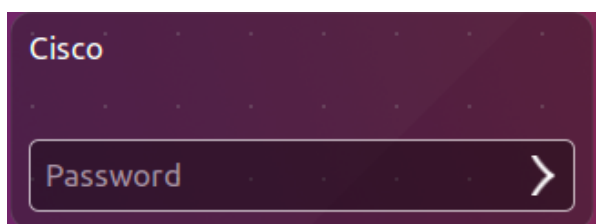
Выполняя эту часть работы, вы научитесь создавать учетные записи пользователей, группы и пароли на локальной хостовой машине.

#### Запуск терминала в Ubuntu.

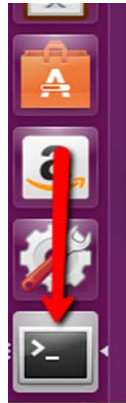
а. Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



- б. Щелкните значок **Terminal** (Терминал), чтобы открыть терминал.



Получите права уровня **root**с помощью команды "**sudo su**". В качестве пароля введите "**password**".

```
cisco@ubuntu:~$ sudo su
```

```
cisco@ubuntu:~$ sudo su
[sudo] password for cisco:
root@ubuntu:/home/cisco#
```

Создайте группу "**HR**" с помощью команды "**groupadd HR**".

```
root@ubuntu:/home/cisco# groupadd HR
```

```
root@ubuntu:/home/cisco# groupadd HR
root@ubuntu:/home/cisco#
```

**Проверка пользователей, групп и паролей**

Убедитесь в том, что новая группа добавлена в файл, содержащий список групп. Для этого введите команду "**cat /etc/group**".

```
root@ubuntu:/home/cisco# cat /etc/group
```

```
root@ubuntu:/home/cisco# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cisco
Bob:x:1002:
Eve:x:1003:
Eric:x:1004:
HR:x:1005:
root@ubuntu:/home/cisco#
```

Новая группа "**HR**"будет добавлена в конец файла **/etc/group**и получит идентификатор 1005.

**Создайте пользователя с именем "jenny".**

```
root@ubuntu:/home/cisco# adduser jenny
```

В качестве пароля введите **lasocial**. Нажмите **Ввод**.

При повторном запросе пароля вновь введите **lasocial**. Нажмите **Ввод**.

В качестве имени введите **Jenny**. Нажмите **Ввод**.

Далее нажимайте клавишу **Ввод** до появления запроса о том, верна ли введенная информация.

Введите **Y** (да) и нажмите **Ввод**.

```
root@ubuntu:/home/cisco# adduser jenny
Adding user `jenny' ...
Adding new group `jenny' (1006) ...
Adding new user `jenny' (1005) with group `jenny' ...
Creating home directory `/home/jenny' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jenny
Enter the new value, or press ENTER for the default
 Full Name []: Jenny
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] Y
```

Добавьте пользователя "jenny" в группу "HR".

```
root@ubuntu:/home/cisco# usermod -G HR jenny
```

```
root@ubuntu:/home/cisco# usermod -G HR jenny
root@ubuntu:/home/cisco#
```

Создайте еще одного пользователя с именем "joe".

```
root@ubuntu:/home/cisco# adduser joe
```

В качестве пароля введите **tooth**. Нажмите **Ввод**.

При повторном запросе пароля вновь введите **tooth**. Нажмите **Ввод**.

В качестве имени введите **Joe**. Нажмите **Ввод**.

Далее нажимайте клавишу **Ввод** до появления запроса о том, верна ли введенная информация.

Введите **Y** (да) и нажмите **Ввод**.

```
root@ubuntu:/home/cisco# adduser joe
Adding user `joe' ...
Adding new group `joe' (1007) ...
Adding new user `joe' (1006) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
 Full Name []: Joe
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] Y
```

Добавьте пользователя "joe" в группу "HR".

```
root@ubuntu:/home/cisco# usermod -G HR joe
```

```
root@ubuntu:/home/cisco# usermod -G HR joe
root@ubuntu:/home/cisco#
```

Убедитесь в том, что созданные пользователи присутствуют в файле "passwd".

```
root@ubuntu:/home/cisco# cat /etc/passwd
```

```
root@ubuntu:/home/cisco# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
eve:x:1003:1003:./home/Eve:
Eric:x:1004:1004:./home/Eric:
jenny:x:1005:1006:Jenny,,,:/home/jenny:/bin/bash
joe:x:1006:1007:Joe,,,:/home/joe:/bin/bash
```

Убедитесь в том, что созданные пользователи присутствуют в файле "shadow".

```
root@ubuntu:/home/cisco# cat /etc/shadow
```

Использование разрешений с использованием символического обозначения

Находясь в Ubuntu, нажмите и удерживайте клавиши CTRL+ALT+F1 до тех пор, пока экран не переключится на терминал tty1.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login:
```

**Примечание.** Если терминал tty1 использовать не удастся, вернитесь в графический пользовательский интерфейс (GUI) хоста, нажав сочетание клавиш CTRL+ALT+F7, и откройте окно терминала в графическом интерфейсе Ubuntu. Введите в командную строку команду **su -l jenny**, затем введите пароль **lasocial**. Перейдите к пункту 4.

```
cisco@ubuntu:~$ su -l jenny
```

```
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

**Примечание.** Если нажатие CTRL+ALT+F7 не приносит результата, попробуйте нажать CTRL+ALT+F8.

Переключившись на терминал, введите "jenny" и нажмите «Ввод».

Введите пароль "lasocial" и нажмите «Ввод».

**Выполнив вход в систему, вы увидите командную строку с подсказкой *jenny@ubuntu:~\$*.**

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

 * Documentation: https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jenny@ubuntu:~$
```

Вы вошли в систему, используя учетную запись обычного пользователя, а не пользователя *root* (суперпользователь), поэтому вместо символа *#* отображается знак доллара.

**Просмотрите ваш текущий рабочий каталог.**

*jenny@ubuntu:~\$ pwd*

```
jenny@ubuntu:~$ pwd
/home/jenny
```

**Перейдите на уровень выше, то есть в каталог *"/home"*.**

*jenny@ubuntu:~\$ cd ..*

```
jenny@ubuntu:~$ cd ..
jenny@ubuntu:/home$
```

**Отобразите все каталоги и разрешения на доступ к ним.**

*jenny@ubuntu:/home\$ ls -l*

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x 3 jenny jenny 4096 Jun 28 23:28 jenny
drwxr-xr-x 2 joe joe 4096 Jun 28 19:18 joe
jenny@ubuntu:/home$
```

В операционной системе Linux разрешения на доступ отображаются в десяти полях, каждое из которых может содержать букву или дефис.

Первое поле содержит дефис, если объект является файлом, или букву *"d"*, если объект является каталогом.

В полях 2–4 отображаются права пользователя.

В полях 5–7 отображаются права группы.

В полях 8–10 отображаются права пользователей категории «остальные» (то есть пользователей, чьи учетные записи не входят в соответствующую группу).



Продолжая действовать от имени пользователя Jenny, перейдите в папку пользователя Joe. Для этого введите команду "cd joe".

```
jenny@ubuntu:/home$ cd joe
```

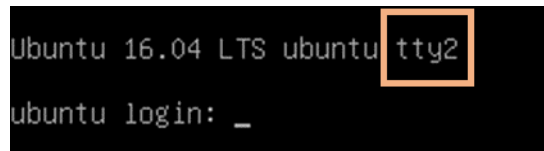
```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$
```

Как видите, вы смогли перейти в домашнюю папку пользователя Joe.

```
jenny@ubuntu:/home/joe$ cd ..
```

```
jenny@ubuntu:/home/joe$ cd ..
jenny@ubuntu:/home$
```

Нажмите CTRL+ALT+F2, чтобы перейти в другой терминал (tty2).



Войдите в систему, указав имя пользователя "root" и пароль "secretpassword".

```
Ubuntu 16.04 LTS ubuntu tty2
ubuntu login: root
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

* Documentation: https://help.ubuntu.com/

15 packages can be updated.
0 updates are security updates.
```

**Примечание.** Если терминал tty2 использовать не удастся, вернитесь в графический пользовательский интерфейс (GUI) хоста, нажав сочетание клавиш **CTRL+ALT+F7**, и откройте окно терминала в графическом интерфейсе Ubuntu. Введите в командную строку команду **sudo -i**. В качестве пароля введите **password**.

```
cisco@ubuntu:~$ sudo -i
[sudo] password for cisco:
root@ubuntu:~#
```

Перейдите в каталог `"/home"`.

```
root@ubuntu:~# cd /home
```

```
root@ubuntu:~# cd /home
root@ubuntu:/home#
```

Измените разрешения на доступ пользователей категории «остальные» к папке пользователя `Joe`, а именно лишите их права выполнения.

```
root@ubuntu:/home# chmod o-x joe
```

```
root@ubuntu:/home# chmod o-x joe
root@ubuntu:/home#
```

Вновь отобразите список каталогов и разрешений на доступ к ним.

```
root@ubuntu:/home# ls -l
```

```
root@ubuntu:/home# ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x 3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr-- 2 joe joe 4096 Jun 28 19:18 joe
root@ubuntu:/home#
```

Как видите, в полях, соответствующих правам доступа пользователей категории «остальные» к папке пользователя `Joe`, отображаются два дефиса.

Нажмите **CTRL+ALT+F1**, чтобы вернуться в предыдущий терминал (`tty1`). Убедитесь в том, что подсказка в командной строке имеет вид `"jenny@ubuntu:/home$"`.

Попытайтесь перейти в папку пользователя `Joe`.

```
jenny@ubuntu:/home$ cd joe
```

```
jenny@ubuntu:/home$ cd joe
-bash: cd: joe: Permission denied
jenny@ubuntu:/home$
```

Как видите, теперь у вас нет разрешения на доступ.

Ниже показаны другие примеры использования команды **chmod**.

| Команда chmod | Результаты                                                            |
|---------------|-----------------------------------------------------------------------|
| chmod u+rwx   | Предоставить пользователю разрешения на чтение, запись и выполнение   |
| chmod u+rw    | Предоставить пользователю разрешения на чтение и запись               |
| chmod o+r     | Предоставить пользователям категории «остальные» разрешение на чтение |
| chmod g-rwx   | Лишить группу разрешений на чтение, запись и выполнение               |

Чтобы завершить сеанс в терминале, введите команду **"exit"** и нажмите «Ввод».

Разрешения с использованием абсолютного обозначения

В терминале **tty1** войдите в систему, указав имя пользователя **"joe"** и пароль **"tooth"**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: joe
Password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-24-generic x86_64)

* Documentation: https://help.ubuntu.com/
```

**Примечание.** Если терминал **tty1** использовать не удастся, вернитесь в графический пользовательский интерфейс (GUI) хоста, нажав сочетание клавиш **CTRL+ALT+F7**, и откройте окно терминала в графическом интерфейсе Ubuntu. Введите в командную строку команду **sudo -l joe**, затем введите пароль **tooth**.

```
jenny@ubuntu:/home$ exit
logout
cisco@ubuntu:~$ su -l joe
Password:
joe@ubuntu:~$
```

Отобразите ваш текущий рабочий каталог.

```
joe@ubuntu:~$ pwd
```

```
joe@ubuntu:~$ pwd
/home/joe
joe@ubuntu:~$
```

Перейдите на уровень выше, то есть в каталог **"/home"**.

```
joe@ubuntu:~$ cd ..
```

```
joe@ubuntu:~$ cd ..
joe@ubuntu:/home$
```

**Отобразите список всех каталогов, содержащихся в текущем рабочем каталоге, и разрешения на доступ к ним.**

joe@ubuntu:/home~\$ ls -l

```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x 3 jenny jenny 4096 Jun 28 23:52 jenny
drwxr-xr-- 3 joe joe 4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

Обратите внимание: пользователи категории «остальные» не имеют права доступа к папке пользователя Joe.

Помимо символьного обозначения, можно использовать абсолютное обозначение разрешений. Абсолютное обозначение разрешений — это обозначение в виде трехзначного восьмеричного числа, кодирующего разрешения пользователя, группы и остальных пользователей.

В следующей таблице представлены все абсолютные обозначения с описанием соответствующих разрешений.

| Количество | Разрешения                  |
|------------|-----------------------------|
| 7          | Чтение, запись и выполнение |
| 6          | Чтение и запись             |
| 5          | Чтение и выполнение         |
| 4          | Чтение                      |
| 3          | Запись и выполнение         |
| 2          | Запись                      |
| 1          | Выполнение                  |
| 0          | None                        |

Команда **chmod 764 examplefile** определяет следующие разрешения на доступ к файлу "examplefile".

Пользователь получает разрешение на чтение, запись и выполнение.

Группа получает разрешение на чтение и запись.

Остальные пользователи получают право чтения.

Каким образом эти разрешения кодируются числом 764?

| Цифра            | Двоичный эквивалент | Разрешение                                                                |
|------------------|---------------------|---------------------------------------------------------------------------|
| 7 (пользователь) | 111                 | 1 — чтение разрешено,<br>1 — запись разрешена<br>1 — выполнение разрешено |
| 6 (группа)       | 110                 | 1 — чтение разрешено,<br>1 — запись разрешена<br>0 — выполнение запрещено |
| 4 (остальные)    | 100                 | 1 — чтение разрешено<br>0 — запись запрещена<br>0 — выполнение запрещено  |

**Измените права доступа к папке пользователя Джо для пользователей категории «остальные», предоставив им права чтения и выполнения без права записи. При этом сам пользователь Джо должен сохранить права чтения, записи и выполнения.**

joe@ubuntu:/home\$ **chmod 705 joe**

```
joe@ubuntu:/home$ chmod 705 joe
joe@ubuntu:/home$
```

**Отобразите разрешения на доступ к текущему каталогу, чтобы убедиться в том, что изменения действительно внесены.**

joe@ubuntu:/home\$ **ls -l**

```
joe@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x 3 jenny jenny 4096 Jun 28 23:52 jenny
drwx---r-x 3 joe joe 4096 Jun 29 00:12 joe
joe@ubuntu:/home$
```

**Перейдите в каталог `/home/joe`.**

joe@ubuntu:/home\$ **cd joe**

```
joe@ubuntu:/home$ cd joe
joe@ubuntu:~$
```

**Создайте текстовый файл с именем `"test.txt"` с помощью команды `touch`.**

joe@ubuntu:~\$ **touch test.txt**

```
joe@ubuntu:~$ touch test.txt
joe@ubuntu:~$
```

- а. Введите команду **exit** и нажмите **Ввод**, чтобы завершить сеанс в терминале.
- б. Оставаясь в терминале **tty1** вновь войдите в систему, используя имя пользователя **jenny** и пароль **lasocial**. Нажмите **Ввод**.

```
Ubuntu 16.04 LTS ubuntu tty1
ubuntu login: jenny
Password:
```

**Примечание.** Если терминал **tty1** использовать не удастся, вернитесь в графический пользовательский интерфейс (GUI) хоста, нажав сочетание клавиш **CTRL+ALT+F7**, и откройте окно терминала в графическом интерфейсе Ubuntu. Введите в командную строку команду **su -l jenny**, затем введите пароль **lasocial**.

```
cisco@ubuntu:~$ su -l jenny
```

```
joe@ubuntu:~$ exit
logout
cisco@ubuntu:~$ su -l jenny
Password:
jenny@ubuntu:~$
```

Перейдите в каталог **"/home"**.

```
jenny@ubuntu:~$ cd /home
```

```
jenny@ubuntu:~$ cd /home
jenny@ubuntu:/home$
```

Отобразите все каталоги и разрешения на доступ к ним.

```
jenny@ubuntu:/home$ ls -l
```

```
jenny@ubuntu:/home$ ls -l
total 12
drwxr-xr-x 17 cisco cisco 4096 Jun 28 18:04 cisco
drwxr-xr-x 3 jenny jenny 4096 Jun 28 23:52 jenny
drwx---r-x 3 joe joe 4096 Jun 29 00:32 joe
jenny@ubuntu:/home$
```

Перейдите в каталог **/home/joe** и отобразите содержимое этого каталога.

```
jenny@ubuntu:/home$ cd joe
```

```
jenny@ubuntu:/home/joe$ ls -l
```

```
jenny@ubuntu:/home$ cd joe
jenny@ubuntu:/home/joe$ ls -l
total 12
-rw-r--r-- 1 joe joe 8980 Jun 28 19:18 examples.desktop
-rw-rw-r-- 1 joe joe 0 Jun 29 00:22 test.txt
jenny@ubuntu:/home/joe$
```

Как видите, вы смогли перейти в папку пользователя Джо и считать информацию о находящихся в нем файлах. Вы видите файл **test.txt**.

**Попробуйте создать файл.**

```
jenny@ubuntu:/home/joe$ touch jenny.txt
```

```
jenny@ubuntu:/home/joe$ touch jenny.txt
touch: cannot touch 'jenny.txt': Permission denied
jenny@ubuntu:/home/joe$
```

Как видите, вы не имеете разрешения на создание файлов.

**Закройте все остальные окна.**

## **Задание 6. Обнаружение угроз и уязвимостей**

### **Задачи**

Выявление угроз и уязвимостей в системе с помощью Nmap (сканер портов/средство для анализа топологии сетевой инфраструктуры).

### **Общие сведения/сценарий**

Network Mapper или Nmap — это утилита с открытым исходным кодом, которая предназначена для обнаружения сетевых ресурсов и проверки средств безопасности. С помощью Nmap администраторы также ведут мониторинг хостов и управляют расписанием обновления сервисов. Nmap позволяет обнаружить присутствующие в сетевой инфраструктуре хосты и определить, какие сервисы, операционные системы, фильтры пакетов или межсетевые экраны работают в настоящий момент.

### **Необходимые ресурсы**

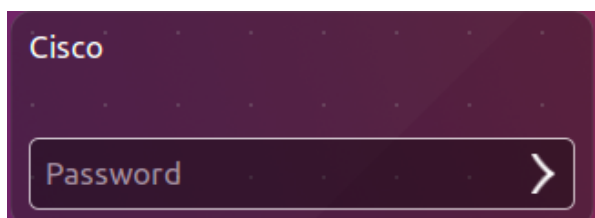
Компьютер с операционной системой Ubuntu 16.0.4 LTS, установленной в виртуальной машине. Можно использовать виртуальную машину, в которой выполнялись предыдущие задания главы 2.

### **Запуск терминала в Ubuntu.**

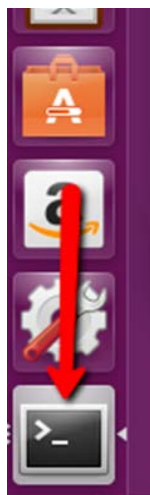
Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



Щелкните значок **Terminal** (Терминал), чтобы открыть терминал.



### Запуск Nmap.

Введите в командную строку следующую команду, которая выполнит базовое сканирование данной системы Ubuntu:

```
cisco@ubuntu:~$ nmap localhost
```

```
cisco@ubuntu:~$ nmap localhost
Starting Nmap 7.01 (https://nmap.org) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

Отображаются результаты сканирования первых 1024 TCP-портов.

Какие TCP-порты открыты в данный момент?

---

### Использование Nmap с правами администратора.

Введите в командную строку терминала следующую команду, чтобы выполнить сканирование UDP-портов компьютера (помня о том, что в Ubuntu учитывается регистр символов). В качестве пароля введите **password**.

```
cisco@ubuntu:~$ sudo nmap -sU localhost
```

```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 (https://nmap.org) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
68/udp open|filtered dhcpc
631/udp open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

Какие UDP-порты открыты?

---

Введите следующую команду в командную строку терминала:

```
cisco@ubuntu:~$ nmap -sV localhost
```

```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 (https://nmap.org) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open telnet Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
cisco@ubuntu:~$
```

Если указан параметр **-sV**, то команда **nmap** выполняет определение версий, результаты которого можно использовать при поиске уязвимостей.

### Получение ключей SSH.

Введите следующую команду в командную строку терминала, чтобы выполнить сканирование на основе сценариев:

```
cisco@ubuntu:~$ nmap -A localhost
```

```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 (https://nmap.org) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_ 256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp open telnet Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
cisco@ubuntu:~$
```

Вы получили ключи SSH для системы хоста. Эта команда выполняет ряд встроенных сценариев Nmap, предназначенных для поиска определенных уязвимостей.

### Справочные материалы

Nmap: <https://nmap.org/>

## Задания по теме «Способы защиты информации ограниченного доступа»

### Задание 7. Применение стеганографии

#### Задачи

Соккрытие документа внутри файла JPEG.

#### Общие сведения/сценарий

Steghide — это стеганографическая утилита с открытым исходным кодом, позволяющая прятать полезные данные в файлах различных типов, включая аудиофайлы и файлы изображений. Вы воспользуетесь этой утилитой, чтобы спрятать файл с данными в файле изображения.

#### Необходимые ресурсы

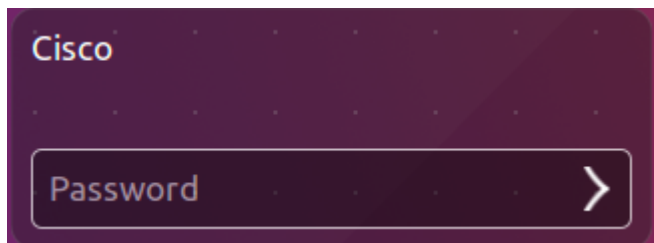
Компьютер с операционной системой Ubuntu 16.04 Desktop LTS, которая установлена в виртуальной машине VirtualBox или VMware.

#### Запуск терминала в Ubuntu.

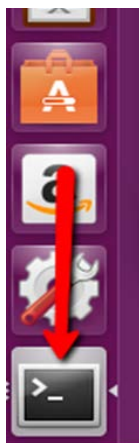
Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



Нажмите значок Terminal (Терминал), чтобы открыть терминал.



#### Запуск Steghide.

Введите в командную строку следующую команду, чтобы перейти в каталог **Downloads**:

```
cisco@ubuntu:~$ cd Downloads/
```

Введите в командную строку команду **libreoffice secret.odt &**.

cisco@ubuntu:~/Downloads\$ **libreoffice secret.odt &**

Какое сообщение содержится в файле **secret.odt**?

---

Изучив сообщение, закройте файл **secret.odt**.

Введите в командную строку команду **gimp keyboard.jpg &**, чтобы просмотреть файл изображения.

cisco@ubuntu:~/Downloads\$ **gimp keyboard.jpg &**

Просмотрев изображение, закройте файл **keyboard.jpg**.

В появившейся командной строке введите команду:

cisco@ubuntu:~/Downloads\$ **steghide embed -cf keyboard.jpg -ef secret.odt**

С помощью этой команды документ **secret.odt** внедряется в файл изображения **keyboard.jpg**.

В качестве фразы-пароля введите **Cisco**. В ответ на повторный запрос фразы-пароля введите ее еще раз.

```
cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt
Enter passphrase:
```

Вы успешно внедрились документ **secret.odt** в файл изображения **keyboard.jpg**.

Откройте файлы **secret.odt** и **keyboard.jpg**. Изменилось ли их содержимое? \_\_\_\_\_

### Проверка скрытого файла.

Введите в командную строку терминала следующую команду:

cisco@ubuntu:~/Downloads\$ **steghide info keyboard.jpg**

```
cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg
"keyboard.jpg":
 format: jpeg
 capacity: 11.9 KB
Try to get information about embedded data ? (y/n)
```

В ответ на запрос введите в командную строку **y** (Да) (не нажимайте **Ввод**).

Введите фразу-пароль **Cisco** и нажмите **Ввод**.

Согласно результату выполнения команды (ниже) файл **secret.odt** зашифрован и сжат.

```
Enter passphrase:
embedded file "secret.odt":
 size: 8.1 KB
 encrypted: rijndael-128, cbc
 compressed: yes
cisco@ubuntu:~/Downloads$
```

### Извлечение скрытого файла.

Введите в командную строку терминала следующую команду:

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
```

Введите фразу-пароль **Cisco** и нажмите **Ввод**.

Введите **y** (Да) в ответ на запрос о замене существующего файла **secret.odt** извлекаемым файлом **secret.odt**.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
Enter passphrase:
the file "secret.odt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.odt".
```

Вы успешно извлекли файл. Откройте извлеченный файл **secret.odt** в LibreOffice.

Удалось ли открыть файл? Изменилось ли содержание секретного сообщения?

---

## Справочные материалы

Steghide: <http://steghide.sourceforge.net/>

Задание по теме «

## Задание 8. Взлом пароля

### Задачи

Выяснение пароля пользователя с помощью утилиты для взлома паролей.

### Общие сведения/сценарий

В системе Linux имеется четыре пользовательских учетных записи: Alice, Bob, Eve и Eric. Вам предстоит выяснить пароли этих учетных записей с помощью утилиты для взлома паролей John the Ripper с открытым исходным кодом.

### Необходимые ресурсы

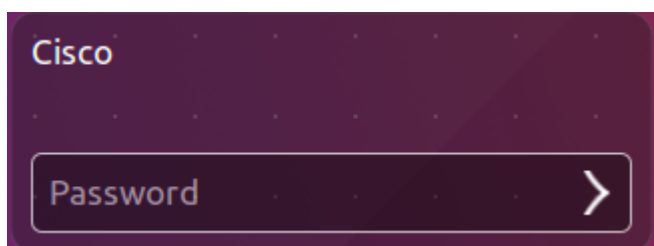
Компьютер с операционной системой Ubuntu 16.04 Desktop LTS, которая установлена в виртуальной машине VirtualBox или VMware.

### Запуск терминала в Ubuntu.

Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



Щелкните значок Terminal (Терминал), чтобы открыть терминал.



### Запускутилиты John the Ripper.

Перейдите в каталог, где находится утилита John the Ripper. Для этого введите в командную строку следующую команду:

```
cisco@ubuntu:~$ cd ~/Downloads/john-1.8.0/run
```

В появившейся командной строке введите команду:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Эта команда объединяет файл /etc/passwd с учетными записями пользователей и файл /etc/shadow с их паролями в новый файл с именем "mypasswd".

### Восстановите пароли.

Введите в терминале следующую команду:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --show mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --show mypasswd
0 password hashes cracked, 5 left
```

Как показано выше, на этом этапе нет взломанных паролей.

В появившейся командной строке введите команду:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --wordlist=password.lst --rules mypasswd --format=crypt
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --wordlist=password.lst --rules mypasswd --format=crypt
```

Программа "John the Ripper" использует готовый словарь **password.lst** со стандартным набором заранее заданных «правил» обработки словаря и извлекает все хеш-коды паролей типа md5crypt и crypt.

Ниже показаны полученные пароли для учетных записей.

```
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1 (Eric)
12345 (Bob)
123456 (Alice)
password (cisco)
password (Eve)
5g 0:00:20:50 100% 0.003998g/s 125.4p/s 376.6c/s 376.6C/s Tnting..Sssing
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

В появившейся командной строке введите команду:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --show mypasswd
```

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$./john --show mypasswd
cisco:password:1000:1000:Cisco,,,:/home/cisco:/bin/bash
Alice:123456:1001:1001::/home/Alice:
Bob:12345:1002:1002::/home/Bob:
Eve:password:1003:1003::/home/Eve:
Eric:password1:1004:1004::/home/Eric:

5 password hashes cracked, 3 left
cisco@ubuntu:~/Downloads/john-1.8.0/run$
```

Сколько паролей взломано?

---

## Справочные материалы

John the Ripper: <http://www.openwall.com/john/>

## Задание по теме «Способы обеспечения целостности данных»

### Задание 9. Использование цифровых подписей

#### Задачи

Получите общее представление о цифровой подписи.

**Часть 1. Демонстрация использования цифровых подписей.**

**Часть 2. Демонстрация проверки цифровых подписей.**

#### Общие сведения/сценарий

Цифровая подпись — это математический способ проверки подлинности и целостности цифрового сообщения. Цифровая подпись является эквивалентом собственноручной. Фактически, цифровые подписи могут быть значительно безопасней. Цифровые подписи предназначены для предотвращения фальсификации и действий от имени другого лица в ходе цифровых коммуникаций. Во многих странах, включая США, цифровая подпись имеет такую же юридическую силу, как и традиционная. Правительство США публикует электронные версии бюджетных документов, законов и законопроектов конгресса с цифровыми подписями.

#### Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

#### Использование цифровых подписей

В этой части для проверки пользователи Alice и Bob на документах будут использоваться веб-сайт. Пользователи Alice и Bob используют одну пару частных и общих ключей RSA. С помощью частного ключа они подписывают юридические документы, которые затем пересылают друг другу. Пользователи Alice и Bob могут проверять подписи друг друга с помощью общего ключа. Они также должны договориться об общей открытой экспоненте для вычислений.

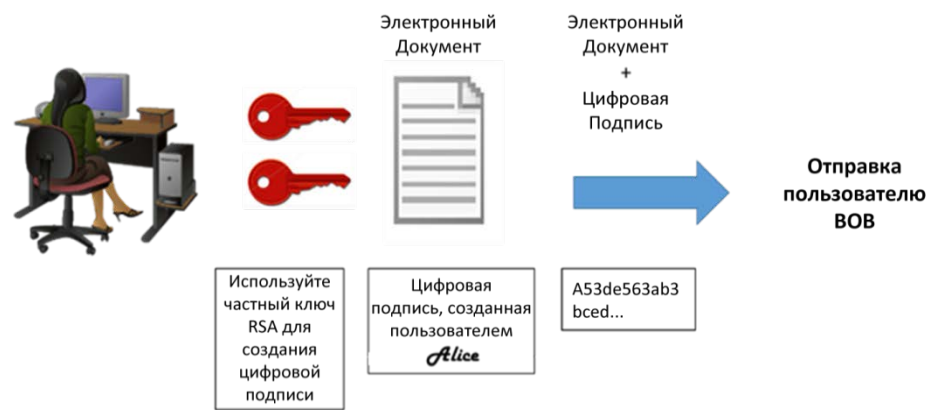
*Таблица 1. Общие и частные ключи RSA*

|                            |                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Общий ключ RSA</b>      | d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549 |
| <b>Закрытый ключ RSA</b>   | 47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcd1fe677dfffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1  |
| <b>Открытая экспонента</b> | 10001                                                                                                                                                                                                                                                            |

#### Подпишите документ.

Пользователь Alice подписывает юридический документ и отправляет его пользователю Bob, используя показанные в таблице выше общий и частный ключи RSA. Далее

пользователю Bob необходимо проверить цифровую подпись пользователя Alice и подтвердить подлинность электронного документа.



**Проверьте цифровую подпись.**

Пользователь Bob получает документ с цифровой подписью, показанной в таблице ниже.

Таблица 2. Цифровая подпись пользователя Alice

| Цифровая подпись пользователя Alice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3<br>0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a<br>0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83<br>0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8<br>0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe<br>0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae<br>0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13<br>0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d |

Нажмите [здесь](#), чтобы использовать онлайн-средство RSA для проверки подлинности цифровой подписи пользователя Alice.

Таблица 3. Онлайн-средство проверки цифровой подписи

## RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

**Public Modulus**  
(hexadecimal):

**Public Exponent**  
(hexadecimal):

**Private Exponent**  
(hexadecimal):

**Text:**

```
d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e
3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d7925
2f5c527b9bc63d83d4ecf4d1d45cbf843e8474bab6c655e9bb6799cba77a47eafa838296474afc24b
eb9c825b73ebf549
```

10001

```
47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e
09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da
038906c84dcdb1fe677dff2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352
df58848adad11a1
```

```
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21
0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e
0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45
0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30
0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f
0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a
0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05
0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d
```

Hexadecimal ☒

Character String ☐

Encrypt

Sign

Decrypt

Verify

Generate

Crack

Скопируйте и вставьте **общий** и **частный** ключи из вышеприведенной таблицы 1 в поля **Public Modulus** и **Private Exponent** на веб-сайте, как показано на рисунке выше.

Используйте для Public Exponent значение 10001.

На веб-сайте вставьте цифровую подпись пользователя Alice из таблицы 2 в поле с меткой text, как показано выше.

Теперь пользователь BOB может проверить цифровую подпись, нажав кнопку **Verify** (Проверить) в центре нижней части веб-сайта. Чья подпись идентифицирована?

### Создайте ответную подпись.

Пользователь Bob получает и проверяет электронный документ и цифровую подпись пользователя Alice. Далее пользователь Bob создает электронный документ и собственную цифровую подпись, используя закрытый ключ RSA из таблицы 1 (обратите внимание: имя пользователя Bob написано заглавными буквами).

Таблица 4. Цифровая подпись пользователя BOB

| Цифровая подпись пользователя BOB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92<br>0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d<br>0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8<br>0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54<br>0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf<br>0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78<br>0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c<br>0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62 |

Пользователь Bob отправляет пользователю Alice электронный документ и цифровую подпись.

### Проверьте цифровую подпись.

Скопируйте и вставьте **общий** и **частный** ключи из вышеприведенной таблицы 1 в поля **Public Modulus** и **Private Exponent** на веб-сайте, как показано на рисунке выше.

Используйте для Public Exponent значение 10001.

На веб-сайте вставьте цифровую подпись пользователя Bob из таблицы 4 в поле с меткой text, как показано выше.

Теперь пользователь Alice может проверить цифровую подпись, нажав кнопку **Verify** (Проверить) в центре нижней части веб-сайта. Чья подпись идентифицирована?

### Создание собственной цифровой подписи

Вы узнали, как используются цифровые подписи. Теперь вы готовы создать собственную цифровую подпись.

### Создайте новую пару ключей RSA.

Откройте веб-сайт и создайте новый набор частных и общих ключей RSA.

Очистите содержимое полей **Public Modulus**, **Private Modulus** и **Text**. С помощью мыши выделите текст и нажмите кнопку Delete на клавиатуре.

В поле Public Exponent используйте значение **10001**.

Создайте новый набор ключей RSA. Для этого нажмите кнопку **Generate** (Создать) справа в нижней части веб-сайта.

Скопируйте новые ключи в таблицу 5.

Таблица 5. Новые ключи RSA

|                         |  |
|-------------------------|--|
| <b>Общий<br/>ключ</b>   |  |
| <b>Частный<br/>ключ</b> |  |

Введите свое полное имя в поле **Text** (Текст) и нажмите кнопку **Sign** (Подписать).

Таблица 6. Личная цифровая подпись

|                                      |  |
|--------------------------------------|--|
| <b>Личная цифро-<br/>вая подпись</b> |  |
|--------------------------------------|--|

### Обмен цифровыми подписями и их проверка

Теперь можно использовать созданную цифровую подпись.

**Сообщите вашему партнеру по выполнению задания новые частный и общий ключи из таблицы 5.**

Запишите закрытый и открытый ключи из таблицы 5 вашего партнера по выполнению задания.

Внесите оба ключа в таблицу ниже.

Таблица 7. Ключи RSA партнеров по выполнению задания

|                     |  |
|---------------------|--|
| <b>Общий ключ</b>   |  |
| <b>Частный ключ</b> |  |

Обменяйтесь своими цифровыми подписями из таблицы 6. Внесите цифровую подпись в таблицу ниже.

|                                                                      |  |
|----------------------------------------------------------------------|--|
| <b>Цифровая под-<br/>пись партнера<br/>по выполнению<br/>задания</b> |  |
|----------------------------------------------------------------------|--|

### Проверка цифровой подписи партнера по выполнению задания

Для проверки цифровой подписи вставьте общий и частный ключи партнера по выполнению задания в соответствующие поля **Public modulus** и **Private modulus** на веб-сайте.

Вставьте цифровую подпись в поле **Text** (Текст).

Нажмите кнопку Verify (Проверить), чтобы проверить цифровую подпись партнера.

Что отображается в текстовом поле?

---

## Задание по теме «Концепция «пять девяток».

### Задание 10. Удаленный доступ

#### Задачи

Сравните использование протоколов SSH и Telnet для доступа к удаленному узлу.

#### Общие сведения/сценарий

Вы будете использовать протоколы SSH и Telnet для удаленного подключения к хосту. SSH — безопасный метод удаленного доступа к хосту SSH. Telnet — небезопасный метод доступа к хосту Telnet.

#### Необходимые ресурсы

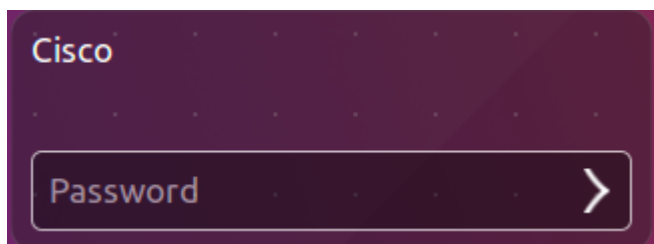
Компьютер с операционной системой Ubuntu 16.04 Desktop LTS, которая установлена в виртуальной машине VirtualBox или VMware.

#### Запустите окно терминала в Ubuntu

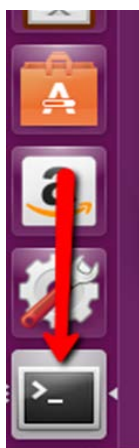
Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



Нажмите значок терминала, чтобы открыть окно терминала.



#### Подключение по протоколу Telnet к локальному хост-компьютеру

В появившейся командной строке введите команду:

```
cisco@ubuntu:~$ telnet localhost
```

Откроется приглашение ко вводу идентификатора пользователя и пароля для учетной записи, существующей на хосте.

Идентификатор пользователя Ubuntu: **cisco**

Пароль: **password**

```
cisco@ubuntu:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04 LTS
ubuntu login: cisco
Password:
Last login: Fri Jun 3 22:22:43 PDT 2016 from localhost on pts/22
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation: https://help.ubuntu.com/

13 packages can be updated.
7 updates are security updates.

cisco@ubuntu:~$
```

Вы успешно вошли в систему на собственном компьютере, используя протокол Telnet.

Чтобы закрыть сеанс Telnet, введите в командной строке следующую команду:

cisco@ubuntu:~\$ **exit**

```
cisco@ubuntu:~$ exit
logout
Connection closed by foreign host.
cisco@ubuntu:~$
```

## Подключение по протоколу SSH к локальному хост-компьютеру

Для доступа к локальному хост-компьютеру по протоколу SSH введите в терминале следующую команду:

cisco@ubuntu:~\$ **ssh localhost**

```
cisco@ubuntu:~$ ssh localhost
cisco@localhost's password:
```

**Примечание.** При первом подключении к системе по протоколу SSH потребуется сохранить в ней ключи безопасности. В открывшемся окне подтвердите продолжение подключения, нажав кнопку **yes** (да).

Для пользователя **cisco** используйте пароль **password**.

```
cisco@localhost's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation: https://help.ubuntu.com/

13 packages can be updated.
7 updates are security updates.

Last login: Fri Jun 3 22:29:58 2016 from localhost
cisco@ubuntu:~$
```

Вы успешно вошли в систему на собственном компьютере, используя протокол SSH.

## Доступ к удаленному узлу

Выберите партнера. На обеих виртуальных машинах выберите мостовое соединение сетевых адаптеров. Для этого в меню **Machine>Settings** (Машина > Настройки) нажмите **Network** (Сеть) и вместо **Attached to: NAT** (Присоединено: NAT) выберите **Attached to: Bridged Adapter** (Присоединено: адаптер Bridged). Дождитесь повторного подключения к сетевой инфраструктуре. Проверьте IP-адрес с помощью следующей команды:

```
cisco@ubuntu:~$ ifconfig
```

```
cisco@ubuntu:~$ ifconfig
ens33 Link encap:Ethernet HWaddr 00:0c:29:f9:1f:e3
 inet addr:192.168.68.130 Bcast:192.168.68.255 Mask:255.255.255.0
 inet6 addr: fe80::8b70:7396:899:7dc1/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:4499 errors:0 dropped:0 overruns:0 frame:0
 TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:774294 (774.2 KB) TX bytes:313660 (313.6 KB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:5900 errors:0 dropped:0 overruns:0 frame:0
 TX packets:5900 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1
 RX bytes:345057 (345.0 KB) TX bytes:345057 (345.0 KB)

cisco@ubuntu:~$
```

**Примечание.** Если новый IP-адрес не получен, щелкните значок сетевой инфраструктуры () (↑↓). Отключите и подключите повторно проводное соединение.

Повторите команды SSH и Telnet, используя вместо локального хост-компьютера IP-адрес партнера.

## Задание по теме «Защита уровней обеспечения кибербезопасности»

### Задание 11. Повышение надежности системы Linux

#### Задачи

Продемонстрируйте использование средства проверки безопасности для повышения надежности системы Linux.

#### Общие сведения/сценарий

Проверка системы на наличие ошибок в конфигурации или отсутствие защиты каких-либо сервисов — важный аспект повышения ее надежности. Lynis — это инструмент проверки безопасности с открытым исходным кодом, которое содержит автоматизированный набор сценариев для тестирования системы Linux.

#### Необходимые ресурсы

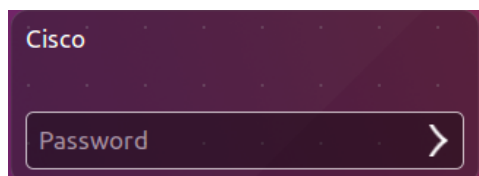
Компьютер с операционной системой Ubuntu 16.04 Desktop LTS, которая установлена в виртуальной машине VirtualBox или VMware.

#### Запуск терминала в Ubuntu.

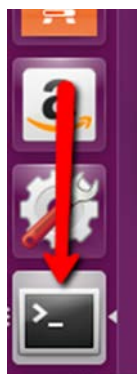
Войдите в Ubuntu, используя следующие учетные данные.

Имя пользователя: **cisco**

Пароль: **password**



Нажмите значок терминала, чтобы открыть окно терминала.



#### Инструмент Lynis

Чтобы перейти в каталог lynis, введите в командной строке следующую команду:

cisco@ubuntu:~\$ **cd Downloads/lynis/**

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

В командной строке введите следующую команду, а затем пароль **password** после приглашения:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info

[Lynis 2.2.0]

#####
comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
Enterprise support and plugins available via CISOfy
#####

[+] Initializing program

- Detecting OS... [DONE]
- Checking profile file (./default.prfl)... [NO UPDATE]
- Program update status...

[+] Helper: update

```

Эта команда проверяет наличие последней версии и обновлений инструмента на момент выполнения задания.

## Запуск инструмента

Введите в терминале следующую команду и нажмите **Enter**:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco

[Lynis 2.2.0]

#####
comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
Enterprise support and plugins available via CISOfy
#####

[+] Initializing program

- Detecting OS... [DONE]

Program version: 2.2.0
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 16.04
Kernel version: 4.4.0
Hardware platform: x86_64
Hostname: ubuntu
Auditor: cisco
Profile: ./default.prfl
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
```

Как показано выше, инструмент начнет проверку, используя в качестве проверяющего пользователя **cisco**.

Примечание. Вы будете получать **предупреждения**.

После каждого этапа нажимайте **Enter** для продолжения. Вы будете получать предупреждения, как в примере ниже.

```
[+] Boot and services

- Service Manager [systemd]
- Checking UEFI boot [DISABLED]
- Checking presence GRUB2 [FOUND]
 - Checking for password protection [WARNING]
- Check running services (systemctl) [DONE]
 Result: found 23 running services
- Check enabled services at boot (systemctl) [DONE]
 Result: found 37 enabled services
- Check startup files (permissions) [OK]

[Press [ENTER] to continue, or [CTRL]+C to stop]
```

Вы будете получать рекомендации, как в примере ниже.

```
[+] Users, Groups and Authentication

- Search administrator accounts [OK]
- Checking for non-unique UIDs [OK]
- Checking consistency of group files (grpck) [OK]
- Checking non unique group ID's [OK]
- Checking non unique group names [OK]
- Checking password file consistency [OK]
- Query system users (non daemons) [DONE]
- Checking NIS+ authentication support [NOT ENABLED]
- Checking NIS authentication support [NOT ENABLED]
- Checking sudoers file [FOUND]
 - Check sudoers file permissions [OK]
- Checking PAM password strength tools [SUGGESTION]
- Checking PAM configuration files (pam.conf) [FOUND]
- Checking PAM configuration files (pam.d) [FOUND]
- Checking PAM modules [FOUND]
- Checking LDAP module in PAM [NOT FOUND]
- Checking accounts without expire date [OK]
- Checking accounts without password [OK]
- Checking user password aging (minimum) [DISABLED]
- Checking user password aging (maximum) [DISABLED]
- Checking expired passwords [OK]
```

Вы получите уведомление о каждой неустойчивой конфигурации, как в примере ниже.

```
[+] Banners and identification

- /etc/motd [NOT FOUND]
- /etc/issue [FOUND]
 - /etc/issue contents [WEAK]
- /etc/issue.net [FOUND]
 - /etc/issue.net contents [WEAK]

[Press [ENTER] to continue, or [CTRL]+C to stop]
```

- е. Вы получите подробные рекомендации по улучшению безопасности, а также итоговую сводку, содержащую местоположение файла журнала.

```
Lynis security scan details:

Hardening index : 56 [#####]
Tests performed : 188
Plugins enabled : 0

Quick overview:
- Firewall [X] - Malware scanner [X]

Lynis Modules:
- Compliance Status [NA]
- Security Audit [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
```

### Просмотр результатов

После завершения работы инструмента просмотрите раздел результатов.

Сколько предупреждений вы получили? \_\_\_\_\_

Сколько рекомендаций вы получили? \_\_\_\_\_

Просмотрите рекомендации и выберите одну из них. Изучите рекомендацию, которую вы могли бы реализовать для устранения проблемы.

Какую рекомендацию вы выбрали?

---

---

---

Какое решение вы предлагаете?

---

---

---

### Справочные материалы

Lynis: <https://cisofy.com/lynis/>

## Список рекомендуемой литературы

### Основная литература:

1. Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах "Информ-2016" : Сборник научных трудов II Международной научно-технической конференции 26-27 мая 2016 г. / ред. кол. В. М. Довгаль, Ю. Н. Быков, Л. С. Крыжевич ; Курск. гос. ун-т, Нац. ун-т Трухильо (Перу), Евраз. нац. ун-т, ВГТУ, РГРУ, ТГУ, БелГТУ, Ч. 1. - Курск : Курск. гос. ун-т, 2016.

### Дополнительная литература:

1. Алгулиев, Р. М. Киберфизические системы: основные понятия и вопросы обеспечения безопасности / Р. М. Алгулиев, Я. Н. Имамвердиев, Л. В. Сухостат [Текст] // Информационные технологии. – 2017.

2. Емельянова, Н. З. Защита информации в персональном компьютере : [учеб. пособие] / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: ФОРУМ, 2009. - 368 с.

3. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 6-е изд., стер. – Москва: Академия, 2012. – 336 с.

4. Козлов, В. Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М.: Горячая линия-ТЕЛЕКОМ, 2002. – 336 с.

5. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс / А.Н. Андрончик. - Екатеринбург: Издательство Уральского университета, 2014. - 179 с. - ISBN 978-5-7996-1201-6