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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы
по дисциплине «Персональная кибербезопасность»

по направлению подготовки 08.03.01 «Строительство»

направленность (профиль) «Проектирование зданий»

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;

Общая характеристика самостоятельной работы студента

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

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

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 заданиям, завести новую тетрадь для конспектирования лекций и выполнения практических и 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 заданиях, 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;

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

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

Порядок выполнения самостоятельной работы

Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой – это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения, излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Самостоятельное изучение тем лекций

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

Задание 1. Идентификация угроз

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения/сценарий

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

Таблица адресации

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

Настройка FTP-сервера

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.

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.

Настройка веб-сервера

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.

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?

_____

_____

Настройка DNS-сервера

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.

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.

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?

_____

_____

Настройка сервера электронной почты

Активация сервисов электронной почты.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **Email/DNS**.

b. Перейдите на вкладку **Services** (Службы) и выберите раздел **EMAIL** (Электронная почта).

c. Включите службы SMTP и POP3 с помощью селективных кнопок, которые находятся в верхней части окна.

Создайте для пользователей учетные записи электронной почты.

a. Создайте доменное имя **cisco.corp**.

b. Создайте учетные записи пользователей с именами **phil**, **sally**, **bob**, **dave**, **mary**, **tim** и **mike**, назначив каждой учетной записи пароль **cisco123**.

Настройка пользовательских клиентов электронной почты.

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

b. Щелкните значок **Email** (Электронная почта) и введите следующую информацию.

Name (Имя): **Sally**

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

Incoming & Outgoing Email Server(s) (сервер (-ы) входящей и исходящей почты): **email.cisco.corp**

Username (имя пользователя): **sally**

Password (пароль): **cisco123**

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

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

_____

_____

Настройка NTP-сервера

Активация службы NTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.

b. Перейдите на вкладку **Services** (Службы) и выберите **NTP**.

c. Включите службу NTP с помощью селективной кнопки в верхней части окна.

Защита службы NTP.

a. Включите функцию аутентификации NTP с помощью соответствующей селективной кнопки.

b. Назначьте ключу **Key 1** пароль **cisco123**.

Настройка AAA-сервера

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.

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 задания	**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**	

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?

Задание № 2. Общение в кибермире

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения

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

Таблица адресации

Устройство	**Частный IP-адрес**	**Общедоступный IP-адрес**	**Маска подсети**	**Сайт**
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ
Сервер резервного копирования файлов	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Передача электронного сообщения от пользователя к пользователю

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

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 отрытого 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 задания	**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**	

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 отрытого текста?
6. Почему протокол SSH считается безопасным средством для удаленного управления устройствами?

Задание № 3. Шифрование файлов и данных

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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 **ОК**.

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 **ОК**.

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 **ftplogin.txt** и нажмите кнопку **ОК**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Bob.

a. Выделите весь текст, содержащийся в файле **ftplogin.txt**, и скопируйте его.

b. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://encipher.it.

c. Поместите курсор в **белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст**.

d. Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки **bobftp123**. Нажмите **Decrypt** (Расшифровать).

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

_____

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

Шаг 1: Удаленное подключение к FTP-серверу.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

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

c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите в командной строке команду **ftp 10.44.1.254**.

d. Введите имя пользователя и пароль, найденные на Шаге 2 в Части 3.

Шаг 2: Загрузите файл на компьютер пользователя Bob.

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

b. Пользователь Mary загрузила на сервер файл clientinfo.txt с зашифрованной информацией о клиентах медицинского учреждения.

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

c. В командную строку с подсказкой **ftp>** введите команду **quit**.

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

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

_____

Учебный вопрос 5: Расшифровка содержимого файла clientinfo.txt

Шаг 1: Получение ключа расшифровки от пользователя Mary.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

c. В окне приложения Email (Электронная почта) нажмите кнопку **Receive** (Получить).

d. Выберите электронное сообщение с темой "Decryption Key" («Ключ расшифровки») и запишите ключ расшифровки ниже.

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

_____

Шаг 2: Расшифровка содержимого файла clientinfo.txt.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **clientinfo.txt** и нажмите кнопку **ОК**.

e. Выделите весь текст, содержащийся в файле **clientinfo.txt**, и скопируйте его.

f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://encipher.it.

g. Поместите курсор в **белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст**.

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

Каково имя первой учетной записи в файле clientinfo.txt?

_____

Предлагаемый способ подсчета баллов

Вопросы задания	**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**	

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?

Задание № 4. Проверка целостности файлов и данных

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

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

Учебные вопросы задания

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

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

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

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Резервный файловый сервер Backup File	—	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Интернет
Mike	10.44.2.101	—	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	—	255.255.255.0	Metropolis Bank HQ
Боб	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

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

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

a. Откройте объект **Gotham Healthcare 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 **Gotham Healthcare 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 **Gotham Healthcare 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 **Gotham Healthcare 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 **Gotham Healthcare 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 **ОК**.

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 **ОК**.

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 задания	**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**	

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?

Задание № 5. WEP/WPA2 PSK/WPA2 RADIUS

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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 сроку 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 **ОК**.

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) > **Wireless Security** (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 сроку 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 **ОК**.

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) > **Wireless Security** (Защита беспроводной сети).

b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2 Personal**.

c. Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. В качестве фразы-пароля введите **ciscosecure**.

d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Подключение клиентских устройств.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Tim**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).

c. Перейдите на вкладку **Connect** (Подключиться) и нажмите кнопку **Refresh** (Обновить).

d. Выберите название беспроводной сети **BranchSite** и нажмите кнопку **Connect** (Подключиться).

e. Введите PSK-ключ **ciscosecure** и нажмите кнопку **Connect** (Подключиться).

f. Повторите шаги **a–e** на компьютере **Mike**.

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

Шаг 1: Настройка идентификатора SSID беспроводной сети.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.

b. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес беспроводного маршрутизатора (**10.44.1.251**). Введите **admin** в качестве имени пользователя и пароля. Щелкните **ОК**.

c. Перейдите на вкладку **Wireless**. Измените идентификатор **SSID** с **DefaultWIFI** на **HQ**.

d. Измените значение параметра Standard Channel (Стандартный канал) на **11 — 2.462GHz**.

e. Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).

f. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

a. Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **Wireless Security** (Защита беспроводной сети).

b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2-Enterprise**.

c. Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. Введите следующие параметры сервера RADIUS:

RADIUS SERVER IP (IP-адрес сервера RADIUS): **10.44.1.252**
Shared Secret (Общий секретный ключ): **ciscosecure**

d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Настройка сервера RADIUS.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.

b. Перейдите на вкладку **Services** (Службы) и выберите раздел **AAA**.

c. Введите следующую информацию в области **Network Configuration** (Конфигурация сети):

Client Name (Имя клиента):.....**HQ**
Client IP (IP-адрес клиента):....**10.44.1.251**
Secret (Ключ): .....**ciscosecure**
ServerType (Тип сервера): .....**Radius**

d. Нажмите **Добавить**.

e. Введите указанные ниже данные в области **User Setup** (Параметры пользователей) и нажмите кнопку **Add** (Добавить), чтобы добавить новое имя пользователя.

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

Шаг 4: Подключение клиентских устройств.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).

c. Перейдите на вкладку **Profiles** (Профили) и нажмите кнопку **New** (Создать).

d. Введите имя профиля **RADIUS** и нажмите кнопку **ОК**.

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 3e.

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

Предлагаемый способ подсчета баллов

Вопросы задания	**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**	

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?

Задание № 6. Настройка транспортного режима VPN

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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.

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: 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 **ОК** 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.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **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**.

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

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

a. Установите соединение с сервером **Private_FTP** объекта **Gotham Healthcare Branch**. Для этого введите команду **ftp 10.44.2.254** в командную строку.

b. Введите имя пользователя **cisco** и пароль **secretkey**, чтобы войти на сервер **Private_FTP**.

c. Выгрузите файл **PrivateInfo.txt** на сервер **Private_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. 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 задания	**Шаги вопроса**	**Максимальное количество баллов**	**Зара ботанные 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**	

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 2c 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.

Задание № 7. Настройка туннельного режима VPN

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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 **FTPupload.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 задания	**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**	

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.

Задание № 8. Резервирование маршрутизаторов и коммутаторов

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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.

a. 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.

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

Какой маршрутизатор теперь работает как шлюз по умолчанию?

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

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

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

a. Выберите узел **Gotham Healthcare Branch** и выберите компьютер **Tim**.

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. 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.

a. В узле **Gotham Healthcare Branch** нажмите коммутатор **S3**.

b. Перейдите на вкладку **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 **Gotham Healthcare Branch** разверните окно, отображающее компьютер пользователя Tim.

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

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?

Задание № 9. Резервирование маршрутизаторов и коммутаторов

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
2. Уметь осуществлять активацию функции Cisco IOS Resilient Configuration.
3. Приобрести способность формировать процедуры для управления информационной безопасностью.

Учебные вопросы задания

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 подсети	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.

a. Выберите узел **Metropolis Bank HQ** и выберите компьютер пользователя **Sally**.

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

Шаг 2: Выполните удаленное подключение к маршрутизатору HQ_Router.

a. 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**.

b. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.

В командной строке должно отображаться следующее:
HQ_Router#

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

Шаг 3: Создайте правовое уведомление на маршрутизаторе HQ_Router.

a. В командной строке HQ_Router# введите команду **configure terminal** для перехода в режим глобальной настройки.

b. 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.
#

c. В командной строке HQ_Router(config)# введите команды **end** и **logout** для завершения соединения с маршрутизатором **HQ_Router**.

d. 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.

a. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.

b. 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.

a. 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 задания	**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	
Вопросы		**40**	
Балл Packet Tracer		**60**	
Общее число баллов		**100**	

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?

Задание № 10. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

Цели задания

В результате настоящего задания и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных заданиях.
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 задания

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

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

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

Таблица адресации

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

Учебный вопрос 1: Подключение к веб-серверу.

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

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 межсетевого экрана не заданы.

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

Предлагаемый способ подсчета баллов

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

Контрольные вопросы

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

Задание № 11. Отработка комплексных практических навыков

Цели задания

В результате настоящего задания 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 Задание 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 рекомендуемой литературы

Список рекомендуемой литературы

Перечень основной литературы:

1. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130.

2. Ванина, А. Г. Персональная кибербезопасность: курс лекций : учебное пособие / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев. — Ставрополь : СКФУ, 2022. — 137 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/386636.

Перечень дополнительной литературы:

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715

2. Кораблева, Е. В. Социально-этические проблемы информационной безопасности : учебно-методическое пособие / Е. В. Кораблева. — Москва : МТУСИ, 2022. — 31 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333719.

3. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические указания для выполнения лабораторных работ по дисциплине «Персональная кибербезопасность» для студентов направления подготовки 15.03.05 Конструкторско-технологическое обеспечение машиностроительных производств, 2025 г (электронный ресурс).

2. Конспект лекций по дисциплине «Персональная кибербезопасность» для студентов направления подготовки 15.03.05 Конструкторско-технологическое обеспечение машиностроительных производств, 2025 г (электронный ресурс).

3. Методические указания по организации и проведению самостоятельной работы по дисциплине «Персональная кибербезопасность» для студентов направления подготовки 15.03.05 Конструкторско-технологическое обеспечение машиностроительных производств, 2025 г (электронный ресурс).

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

1 Автоматизированная информационно-библиотечная система «Фолиант» http://catalog.ncfu.ru/catalog/ncfu

2 Сетевая академия Cisco Networking Academy - https://www.netacad.com/ru/

3 Электронно-библиотечная система IPR BOOKS - http://www.iprbookshop.ru/

4 Электронные образовательные ресурсы - http://www.ncfu.ru/index.php?do=static&page=elektronnye-obrazovatelnye-resursy