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

Методические указания

по выполнению лабораторных работ
по дисциплине «ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ»
для студентов направления подготовки
15.03.05 Конструкторско-технологическое обеспечение машиностроительных производств
Направленность (профиль) Технология машиностроения

Ставрополь 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
Указания по технике безопасности при выполнении занятий 5
Тема 1. Кибербезопасность — мир экспертов и преступников 6
Занятие 1. Насколько рискованно ваше поведение в Интернете 6
Задачи 6
Исходные данные/сценарий 6
Часть 1: Изучение условий политик обслуживания 6
Часть 2: Анализ вашего поведения в Интернете 7
Вопросы для повторения 8
Тема 2. Куб кибербезопасности 9
Занятие 2. Игра «Подбор» по теме «Волшебный куб кибербезопасности» на веб-сайте Quizlet 9
Тема 3. Свойства противодействия угрозам кибербезопасности 11
Занятие 3. Идентификация угроз 11
Тема 4. Угрозы кибербезопасности, уязвимости и атаки 14
Занятие 4. Задачи профессионалов в сфере кибербезопасности 14
Тема 5. Способы защиты информации ограниченного доступа 18
Занятие 5. Кому принадлежат ваши данные 18
Задачи 18
Исходные данные/сценарий 18
Необходимые ресурсы 18
Часть 3: Изучение условий политик обслуживания 18
Часть 4: А вы знаете, под чем подписываетесь? 19
Тема 6. Способы обеспечения целостности данных 20
Занятие 6. Установка виртуальной машины на ПК 20
Задачи 20
Общие сведения/сценарий 20
Необходимые ресурсы 20
Часть 1: Подготовка хост-компьютера к виртуализации 20
Шаг 1: Загрузка и установка VirtualBox 20
Шаг 2: Загрузка файла образа виртуальной машины 21
Часть 2: Импорт виртуальной машины в реестр устройств приложения VirtualBox 21
Шаг 1: Импорт виртуальной машины в VirtualBox 21
Шаг 2: Запуск виртуальной машины и вход в операционную систему 21
Шаг 3: Начало работы с виртуальной машиной 22
Вопросы для обсуждения 22
Тема 7. Концепция «пять девяток» 23
Занятие 7. Создание и хранение надежных паролей 23
Задачи 23
Исходные данные/сценарий 23
Необходимые ресурсы 23
Часть 5: Создание надежного пароля 23
Часть 6: Надежное хранение паролей 24
Часть 7: Что же тогда надежный пароль? 25
Тема 8. Защита уровней обеспечения кибербезопасности 26
Занятие 8. Резервное копирование данных 26
Тема 9. Специалисты в области кибербезопасности 29
Занятие 9. Поиск вакансий в сфере кибербезопасности 29
Задачи 29

Общие сведения/сценарий 29
Необходимые ресурсы 29
Часть 1: Изучение вакансий в сфере кибербезопасности 29
Шаг 1: Изучение вакансий в сфере кибербезопасности. 29
Шаг 2: Изучение уровня оплаты труда в сфере кибербезопасности 30
Часть 2: Требования работодателей к специалистам в сфере кибербезопасности 30
Шаг 1: Изучение веб-сайта CareerBuilder. 30
Шаг 2: Поиск вакансий в государственных учреждениях США. 31
Список рекомендуемой литературы 32

ВВЕДЕНИЕ

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

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

Задачами дисциплины являются:

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

Методические указания содержат 9 лабораторных занятий, подлежащих выполнению студентами.

Каждое лабораторное занятие состоит из следующих разделов:

- наименование занятия;
- цель занятия;
- общие сведения/сценарий;
- необходимые ресурсы;
- теоретический материал;
- методические пояснения и рекомендации по выполнению практического занятия;
- содержание отчета.

Методические указания содержат список литературы, общий для всех занятий. Методические указания выступают в качестве информационного и практического источника и могут быть использованы для очного и дистанционного обучения.

Указания по технике безопасности при выполнении лабораторных работ

Требования безопасности перед началом работ

– ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

– убедиться в отсутствии видимых повреждений на рабочем месте;

– разместить на столе тетради, учебные пособия так, чтобы они не мешали работе на компьютере;

– включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или сотрудника лаборатории.

Требования безопасности во время работы

– ЗАПРЕЩАЕТСЯ: присоединять или отсоединять кабели, трогать разъемы, провода и розетки, открывать системный блок, пытаться самостоятельно устранять неисправности в работе оборудования, приносить и запускать компьютерные игры;

– выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данной работе;

– подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

– при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или сотруднику лаборатории;

Требования безопасности по окончании работы

– доложить руководителю занятий или сотруднику лаборатории о завершении работ;

– привести в порядок и сдать рабочее место сотруднику лаборатории, и доложить руководителю занятий о сдаче.

Тема 1. Кибербезопасность – мир экспертов и преступников
Занятие 1. Насколько рискованно ваше поведение в Интернете

Задачи

Проанализировать свои действия в Интернете, которые могут скомпрометировать вашу безопасность или конфиденциальность.

Исходные данные/сценарий

Интернет — это агрессивная среда, и вы должны вести себя очень осмотрительно, чтобы ваши данные не были скомпрометированы. Злоумышленники чрезвычайно изобретательны и используют множество способов, чтобы провести пользователей. В ходе этой лабораторной работы вы узнаете, что такое рискованное поведение в Интернете, и получите рекомендации о том, как обезопасить себя в сети.

Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

Часть 1: Изучение условий политик обслуживания

Честно ответьте на вопросы ниже и запишите, сколько баллов принес вам каждый ответ. Суммируйте все баллы для получения общей оценки и перейдите ко второй части, чтобы проанализировать свое поведение в Интернете.

a. Какого рода информацию вы публикуете на сайтах социальных сетей? _____
   1) Все что угодно, я пользуюсь социальными сетями для общения с друзьями и родственниками (3 балла).
   2) Статьи и новости, которые я нашел или прочитал (2 балла).
   3) По-разному; я всегда выбираю, чем и с кем мне делиться (1 балл).
   4) Ничего, я не пользуюсь соцсетями (0 баллов).

b. Когда вы создаете новую учетную запись в онлайн-сервисе, вы: _____
   1) повторно используете тот же пароль, которым пользовались для других сервисов, чтобы его легче было запомнить (3 балла);
   2) создаете как можно более простой пароль, чтобы его можно было легко запомнить (3 балла);
   3) создаете очень сложный пароль и храните его в менеджере паролей (1 балл);
   4) создаете новый пароль, который похож, но все же отличается от пароля, используемого для другого сервиса (1 балл);
   5) создаете абсолютно новый надежный пароль (0 баллов).

c. Если вы получили эл. письмо со ссылками на другие сайты: _____
   1) вы не нажимаете на ссылку, потому что вы никогда не открываете ссылки, отправленные по эл. почте (0 баллов);
   2) вы нажимаете на ссылки, потому что почтовый сервер уже проверил это письмо (3 балла);
   3) вы нажимаете на все ссылки, если письмо пришло от человека, которого вы знаете (2 балла);
   4) вы наводите курсор мыши на ссылки, чтобы проверить URL-адрес, прежде чем нажать на ссылку (1 балл).

d. Вы зашли на веб-сайт, и на нем появилось всплывающее окно, в котором написано, что ваш компьютер подвергается опасности и, чтобы его защитить, вы должны загрузить и установить программу диагностики. _____
   1) Вы нажимаете на ссылку, загружаете и устанавливаете эту программу, чтобы обезопасить свой компьютер (3 балла).
   2) Вы изучаете всплывающее окно и наводите курсор на ссылку, чтобы удостовериться в ее подлинности (3 балла).
   3) Вы игнорируете сообщение, не нажимаете на ссылку, не загружаете программу и уходите с этого веб-сайта (0 баллов).

e. Когда вам нужно войти на веб-сайт вашего банка, чтобы выполнить какое-либо действие, вы: _____
   1) сразу же вводите данные для входа (3 балла);

2) вы проверяете URL-адрес, чтобы удостовериться, что это действительно ваш банк, прежде чем ввести какую-либо информацию (0 баллов);
3) вы не пользуетесь онлайн-банкингом и другими финансовыми онлайн-сервисами (0 баллов).

f. Вы прочитали о какой-либо программе и решили ей воспользоваться. Вы ищете ее в Интернете и находите пробную версию на неизвестном сайте. Ваши действия: _____
1) быстро загружаете и устанавливаете программу (3 балла);
2) прежде чем ее установить, ищете более подробную информацию о создателе программы (1 балл);
3) не загружаете и не устанавливаете программу (0 баллов).

g. По пути на работу вы нашли USB-накопитель. Ваши действия. _____
1) Берете его и вставляете в свой компьютер, чтобы посмотреть, что на нем записано (3 балла).
2) Берете его и вставляете в свой компьютер, чтобы полностью стереть его содержимое, прежде чем заново использовать (3 балла).
3) Берете его и вставляете в свой компьютер, чтобы запустить сканирование антивирусной программой, прежде чем использовать его для своих файлов (3 балла).
4) Не берете его (0 баллов).

h. Вам необходимо подключиться к Интернету, и вы нашли открытую точку доступа Wi-Fi. Ваши действия: _____
1) подключаетесь к ней и пользуетесь Интернетом (3 балла);
2) не подключаетесь к ней и дожидаетесь доверенного подключения (0 баллов);
3) подключаетесь к ней и через VPN подключаетесь к доверенному серверу, прежде чем оправить любую информацию (0 баллов).

Часть 2: Анализ вашего поведения в Интернете

Чем выше итоговая оценка, тем менее безопасно ваше поведение. Цель — обеспечить абсолютную безопасность, осознанно и осторожно выполняя любые действия в Интернете. Это очень важно, ведь для компрометации вашего компьютера и данных достаточно всего одной ошибки.

Суммируйте баллы, набранные в первой части. Запишите общую оценку. _____

0: вы очень осторожны в Интернете и можете чувствовать себя в безопасности.

0–3: вы действуете достаточно осторожно, но, чтобы обеспечить полную безопасность, должны быть еще внимательнее.

3–17: ваше поведение в сети небезопасно, вы подвергаете себя риску компрометации.

18 и больше: вы совершенно не соблюдаете правил безопасности и будете скомпрометированы.

Ниже приводится несколько важных советов по обеспечению безопасности в сети.

a. Чем больше информации о себе вы выкладываете в социальных сетях, тем больше злоумышленники знают о вас. Соответственно, чем больше у них будет информации, тем изощреннее будет их целевая атака. Например, если вы поделились с миром новостью о том, что ходили на автогонки, злоумышленник может прислать вам вредоносное эл. письмо от имени компании, которая продала вам билеты на это событие. Так как вы только что посетили это мероприятия, такое эл. письмо может не вызвать у вас подозрений.

b. Повторно использовать пароли недопустимо. Если вы использовали пароль для какого-либо сервиса, который был атакован злоумышленниками, они могут с успехом воспользоваться вашим паролем для доступа и на другие сервисы.

c. Эл. письма очень легко подделать так, чтобы они выглядели абсолютно официальными. Поддельные письма часто содержат ссылки на вредоносные сайты или ПО. Руководствуйтесь общим правилом: не нажимайте на ссылки из эл. письма.

d. Не принимайте неизвестное ПО, особенно если оно находится на какой-то веб-странице. Маловероятно, что на этой веб-странице будет находиться официальное обновление для вашего ПО. Настоятельно рекомендуется закрыть браузер и воспользоваться инструментами операционной системы для проверки наличия обновлений.

e. Вредоносные веб-страницы могут легко выглядеть как веб-страницы финансовых учреждений или банков. Прежде чем нажать на ссылку или предоставить любую информацию, еще раз проверьте URL-адрес, чтобы быть уверенным, что он ведет на правильную веб-страницу.

f. Если вы разрешили установку программы на своем компьютере, значит, вы предоставили ей массу возможностей. Прежде чем запустить программу, подумайте и все взвесьте. Проверьте и убедитесь, что компания или частное лицо, выпускающие эту программу, действительно являются ее законным автором. Кроме того, загружайте программы только с официальных веб-сайтов компаний или частных лиц.

g. USB-накопители и флешки включают небольшой контроллер, который позволяет компьютерам связываться с ними. Существует возможность инфицировать этот контроллер и проинструктировать его установить вредоносное ПО на компьютер. Так как это вредоносное ПО размещается на самом USB-контроллере, а не в области данных, его нельзя удалить форматированием и его не сможет обнаружить ни одно антивирусное сканирование.

h. Злоумышленники часто разворачивают поддельные точки доступа Wi-Fi, чтобы заманить пользователей. Так как злоумышленник имеет доступ ко всей информации, обмен которой происходит через скомпрометированную точку доступа, подключение пользователя к такой точке доступа несет в себе определенный риск. Никогда не пользуйтесь неизвестными точками доступа Wi-Fi, не зашифровав свой трафик через VPN. Никогда не передавайте конфиденциальные данные, например номера кредитной карты, подключаясь к неизвестной сети (проводной или беспроводной).

Вопросы для повторения

Вы проанализировали свое поведение в Интернете. Каким образом вы должны его изменить, чтобы защитить себя?

_____

_____

_____

_____

Тема 2. Куб кибербезопасности

Занятие 2. Игра «Подбор» по теме «Волшебный куб кибербезопасности» на веб-сайте Quizlet

Задачи

Изучение трех измерений волшебного куба кибербезопасности и элементов этих измерений.

Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

Общие сведения/сценарий

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

Первое измерение. **Принципы кибербезопасности: КЦД**
Конфиденциальность. Исключить намеренное или случайное раскрытие конфиденциальной информации.
Целостность. Исключить намеренное или случайное изменение информации, в результате которого может быть нарушена ее надежность.
Доступность. Обеспечить надежный и своевременный доступ авторизованных лиц к информации и информационным системам.
Второе измерение. **Состояния информации (данных)**
Хранение. Данные в состоянии покоя (хранятся в памяти или на флеш-диске).
Передача. Передача данных между различными системами.
Обработка. Выполнение операций над данными (изменение, резервное копирование, корректирование и др.).
Третье измерение. **Механизмы и контрмеры безопасности**
Политика и практические методы. Административный контроль (политика информационной безопасности, процедуры, указания, руководящие директивы и др.).
Человеческие факторы. Каждый пользователь информационной системы должен понимать свою роль и ответственность. Необходимы соответствующие образовательные программы.
Технологии. Программные и аппаратные решения, предназначенные для защиты информационных систем (антивирусы, межсетевые экраны, системы обнаружения/предотвращения вторжений и др.).

Обзор веб-сайта Quizlet

Перейдите на веб-сайт Quizlet (https://quizlet.com/135368588/cybersecurity-essentials-flash-cards/) и просмотрите материал «Основы кибербезопасности — волшебный куб кибербезопасности». Для просмотра не обязательно иметь учетную запись на этом веб-сайте.

Просмотрите список терминов и определений.

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

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

Перенесите каждый термин к соответствующему определению.

Тема 3. Свойства противодействия угрозам кибербезопасности
Занятие 3. Идентификация угроз

Задачи

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

Часть 1. Изучение угрозы, исходящей от кибератак

Часть 2. Триада КЦД

Общие сведения/сценарий

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

Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

Изучение угрозы, исходящей от кибератак

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

Исследование угроз.

Шаг 1 посвящен исследованию угроз.

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

_____

_____

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

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

Изучение недавних атак.

a. Последствия и масштаб недавних кибератак обеспокоили многих руководителей в частных и государственных структурах. Нажмите здесь (http://www.information-age.com/technology/security/123460657/top-10-most-devastating-cyber-hacks-2015), чтобы прочесть о десяти наиболее разрушительных кибератаках 2015 г.

   Скольких людей затронула утечка данных в Управлении кадровой службы США?

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

Конфиденциальность, целостность и доступность

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

Изучение триады КЦД

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

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

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

_____

_____

Изучение кибератак.

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

_____

_____

Тема 4. Угрозы кибербезопасности, уязвимости и атаки
Занятие 4. Задачи профессионалов в сфере кибербезопасности

Задачи

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

Часть 1. Защита ваших данных

Часть 2. Усиление безопасности вашей учетной записи Google

Общие сведения/сценарий

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

Видеоролики:

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

Ключ безопасности (https://www.youtube.com/watch?v=LUHOs_ggvi4)

Необходимые ресурсы

ПК или мобильное устройство с доступом к Интернету

Защита ваших данных

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

Откройте браузер и просмотрите следующий видеоролик:

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

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

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

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

Выявление уязвимостей, связанных с данными.

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

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

Усиление безопасности вашей учетной записи Google

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

Откройте браузер и просмотрите следующий видеоролик:

Ваш ключ: проще, быстрее и безопаснее (https://www.youtube.com/watch?v=LUHOs_ggvi4)

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

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

---

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

Исключение несанкционированного доступа к учетной записи Gmail.

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

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

Проверка активности учетной записи Gmail.

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

Войдите в свою ученую запись Gmail.

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

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

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

роль, иначе неавторизованные пользователи смогут восстановить доступ к вашей учетной записи.

Тема 5. Способы защиты информации ограниченного доступа
Занятие 5. Кому принадлежат ваши данные

Задачи

Понять, кому принадлежат ваши данные, когда они не хранятся в локальной системе.

Часть 1. Изучение условий политик обслуживания

Часть 2. А вы знаете, под чем подписываетесь?

Исходные данные/сценарий

Социальные сети и онлайн-хранилища стали неотъемлемой частью жизни людей. Мы обмениваемся файлами, фотографиями и видео с друзьями и родственниками. Мы проводим собрания и взаимодействуем онлайн в рабочем пространстве с людьми, которые находятся от нас за многие километры. Хранение данных больше не ограничивается только устройствами, доступными локально. Географическое расположение устройств хранения больше не препятствует хранению или резервному копированию данных в удаленные местоположения.

В этой лабораторной работе вы изучите юридические соглашения, требуемые для пользования различными онлайн-сервисами. Вы также узнаете об отдельных способах защиты ваших данных.

Необходимые ресурсы

- ПК или мобильное устройство с доступом в Интернет

Часть 3: Изучение условий политик обслуживания

Если вы пользуетесь онлайн-сервисами для хранения данных или общения с друзьями и родственниками, вы наверняка заключили соглашение с провайдером. Условия обслуживания, которые могут также называться Условиями использования или просто Условиями, — это юридически обязывающий договор, устанавливающий правила взаимоотношений между вами, провайдером и другими лицами, пользующимися этим сервисом.

Перейдите на веб-сайт используемого вами онлайн-сервиса и найдите соглашение об условиях использования. Ниже мы приводим список наиболее популярных социальных сетей и онлайн-сервисов хранения данных.

Социальные сети

Например, Pinterest: https://about.pinterest.com/en/terms-service

Онлайн-хранилища

Например, icloud: https://www.apple.com/legal/internet-services/icloud/en/terms.html

Dropbox: https://www.dropbox.com/terms2014

OneDrive: http://windows.microsoft.com/en-us/windows/microsoft-services-agreement

Ознакомьтесь с условиями и ответьте на следующие вопросы.

a. Есть ли у вас учетная запись у какого-либо провайдера онлайн-услуг? Если да, читали ли вы Условия соглашения?

_____

_____

b. Какова политика использования данных?

_____

_____

c. Каковы настройки конфиденциальности?

_____

_____

d. Какова политика безопасности?

_____

_____

e. Какие вы имеете права на свои данные? Можете ли вы запросить копию данных?

_____

_____

f. Что может делать провайдер с данными, которые вы загрузили?

_____

_____

g. Что происходит с данными, когда вы удаляете учетную запись?

_____

_____

Часть 4: А вы знаете, под чем подписываетесь?

Вы создали учетную запись и приняли Условия обслуживания. А вы знаете, под чем вы фактически подписались?

Во второй части мы узнаем, как провайдеры могут интерпретировать и использовать Условия обслуживания.

Найдите в Интернете информацию о том, как можно интерпретировать Условия обслуживания.

Ниже мы приводим несколько примеров статей, с которых можно начать.

iCloud

http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html

Dropbox

http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/

Прочитайте статьи и ответьте на следующие вопросы.

a. Что вы можете сделать, чтобы защитить себя?

_____

_____

b. Что вы можете сделать, чтобы защитить свою учетную запись и свои данные?

_____

_____

Тема 6. Способы обеспечения целостности данных
Занятие 6. Установка виртуальной машины на ПК

Задачи

Часть 1. Подготовка компьютера для виртуализации
Часть 2. Импорт виртуальной машины в реестр устройств приложения VirtualBox

Общие сведения/сценарий

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

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

Необходимые ресурсы

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

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

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

Часть 1: Подготовка хост-компьютера к виртуализации

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

Шаг 1: Загрузка и установка VirtualBox

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

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

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

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

Шаг 2: Загрузка файла образа виртуальной машины

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

Нажмите здесь, чтобы загрузить файл образа виртуальной машины.

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

Часть 2: Импорт виртуальной машины в реестр устройств приложения VirtualBox

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

Шаг 1: Импорт виртуальной машины в VirtualBox

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

b. Откроется новое окно. Укажите местоположение файла .OVA.

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

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

Шаг 2: Запуск виртуальной машины и вход в операционную систему

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

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

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

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

Имя пользователя: cisco

Пароль: password

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

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

Шаг 3: Начало работы с виртуальной машиной

Виртуальная машина Ubuntu_CyberEss, которую вы только что установили, предназначена для выполнения лабораторных работ в операционной системе Ubuntu. Изучите следующие значки.

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

- Поиск
- Файловый менеджер
- Веб-браузер Firefox
- LibreOffice Writer, LibreOffice Calc, LibreOffice Impress
- Центр приложений Ubuntu
- Amazon
- Установка системы
- Терминал
- Корзина

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

   Какой IP-адрес назначен виртуальной машине?

   _____

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

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

   _____

   _____

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

Вопросы для обсуждения

Назовите преимущества и недостатки виртуальных машин.

_____

_____

_____

_____

Тема 7. Концепция «пять девяток»
Занятие 7. Создание и хранение надежных паролей

Задачи

Понять, что такое надежный пароль.

Часть 1. Понятие надежного пароля

Часть 2. Надежно ли хранятся ваши пароли?

Исходные данные/сценарий

Пароли используются повсеместно для регулирования доступа к ресурсам. Злоумышленники используют самые различные способы для того, чтобы узнать пароли пользователей и получить несанкционированный доступ к ресурсам или данным.

Чтобы защитить себя, важно понимать, что представляет собой надежный пароль и как его следует хранить.

Необходимые ресурсы

- ПК или мобильное устройство с доступом в Интернет

Часть 5: Создание надежного пароля

Чтобы создать надежный пароль, необходимо соблюсти 4 основных требования, перечисленных в порядке важности.

1) Пользователь должен легко запомнить пароль.
2) Другие лица не смогут быстро угадать этот пароль.
3) Никакая программа не сможет быстро угадать/подобрать пароль.
4) Пароль должен быть сложным, содержать цифры, символы и заглавные и строчные буквы.

В соответствии с приведенным выше списком первое требование, возможно, является самым важным, потому что вам будет необходимо запомнить этот пароль. Например, пароль **#4ssFrX^-aartPOknx25_70!xAdk<d!** считается надежным, потому что удовлетворяет всем трем последним требованиям, но его очень сложно запомнить.

Большинство организаций требует, чтобы пароль состоял из комбинации цифр, символов и заглавных и строчных букв. Пароли, соответствующие этой политике, вполне допустимы, но только если пользователю будет легко их запомнить. Ниже приводится пример политики составления пароля, действующей в типичной организации.

- Пароль должен быть длиной минимум 8 символов.
- Пароль должен включать заглавные и строчные буквы.
- Пароль должен содержать цифру.
- Пароль должен содержать символ (не букву и не цифру).

Проанализируйте характеристики надежного пароля и общую политику создания пароля, представленную выше. Почему данная политика противоречит первым двум пунктам? Поясните ответ.

_____

_____

_____

_____

_____

_____

Для создания надежных паролей мы рекомендуем составлять цепочку из четырех или более случайных слов и связывать их друг с другом. Пароль **televisionfrogbootschurch** надежнее, чем **J0n@than#81**. Несмотря на то, что второй пароль полностью соответствует приведенным

выше политикам, программы для взлома пароля достаточно эффективны, чтобы вычислить такой тип пароля. Хотя пароль **televisionfrogbootschurch** не будет принят большинством политик создания паролей, на самом деле он намного надежнее, чем второй пароль. Пользователю проще его запомнить (особенно потому, что он связан с образом), он очень длинный, а сам набор слов настолько случаен, что делает задачу его взлома практически неосуществимой.

Используя онлайн-инструмент генерации паролей, создайте пароли на основе политики, описанной выше.

a. Откройте веб-браузер и перейдите по ссылке: http://passwordsgenerator.net.

b. Выберите варианты в соответствии с заданной политикой создания паролей.

c. Создайте пароль.

   Легко ли запомнить созданный пароль?

   _____

   _____

   При использовании онлайн-инструмента для создания паролей пароли создаются на основе случайных слов. Так как слова слиты вместе, их нельзя вычленить как отдельные словарные статьи (т. е. слова из словаря).

d. Откройте веб-браузер и перейдите по ссылке: http://preshing.com/20110811/xkcd-password-generator/.

e. Создайте случайный словарный пароль, нажав кнопку **Generate Another! (Создать другой!)** вверху веб-страницы.

f. Легко ли запомнить созданный пароль?

   _____

   _____

Часть 6: Надежное хранение паролей

Если пользователь решит использовать менеджер паролей, первое правило надежного пароля будет нарушено, так как пользователю нужно будет все время обращаться к менеджеру паролей. Заметим, что отдельные пользователи хранят свои пароли только в своей памяти. Менеджеры паролей (как локальные, так и удаленные) должны иметь хранилище паролей, а оно может быть скомпрометировано.

Хранилище менеджера паролей должно быть надежно зашифровано, а доступ к нему должен тщательно контролироваться. Облачные менеджеры паролей обеспечивают бесперебойный доступ для своих пользователей в любое время через мобильные приложения на телефонах и веб-интерфейсы.

Популярным менеджером паролей является Last Pass.

Создайте пробную учетную запись Lastpass.

a. Откройте веб-браузер и перейдите по ссылке: https://lastpass.com/.

b. Щелкните **Получить LastPass Free (Get LastPass Free)**, чтобы создать пробную учетную запись.

c. Заполните поля в соответствии с инструкцией.

d. Задайте мастер-пароль. С этим паролем вы будете входить в свою учетную запись LastPass.

e. Загрузите и установите клиент LastPassдля своей операционной системы.

f. Откройте клиент и войдите в него со своим мастер-паролем LastPass.

g. Изучите менеджер паролей LastPass.

   Когда вы добавляете пароли в Lastpass, где они хранятся?

   _____

   Помимо вас, к вашим паролям имеет доступ как минимум еще одно лицо. Кто это лицо?

   _____

Если все пароли хранятся в одном месте, наверняка в этом есть недостатки. Подумайте, какие?

_____

_____

_____

Часть 7: Что же тогда надежный пароль?

Опираясь на характеристики надежного пароля, приведенные в начале этой лабораторной работы, выберите пароль, который было бы легко запомнить, но трудно подобрать. Сложные пароли вполне допустимы, если только они не противоречат более важным требованиям, например возможности легко их запоминать.

При использовании менеджера паролей необходимость в легком запоминании пароля отпадает.

Итак, резюме.

Выбирайте пароль, который можете запомнить.

Выбирайте пароль, который ни у кого не будет ассоциироваться лично с вами.

Выбирайте разные пароли и никогда не используйте один и тот же пароль для разных сервисов.

Сложные пароли использовать можно, только если их будет просто запомнить.

Тема 8. Защита уровней обеспечения кибербезопасности
Занятие 8. Резервное копирование данных

Задачи

Создать резервную копию данных пользователя.

Часть 1. Использование локального внешнего диска для резервного копирования данных

Часть 2. Использование удаленного диска для резервного копирования данных

Исходные данные/сценарий

Важно создать стратегию резервного копирования, включающую восстановление данных персональных файлов. Сейчас доступно множество разных инструментов резервного копирования, но в данной лабораторной работе для резервного копирования на локальные внешние диски мы будем пользоваться программой архивации Microsoft Backup Utility. Во второй части этой лабораторной работы мы будем пользоваться сервисом Dropbox, чтобы скопировать данные на удаленный или облачный диск.

Необходимые ресурсы

ПК или мобильное устройство с доступом в Интернет

Часть 1: Резервное копирование на локальный внешний диск

Шаг 1: Использование средств резервного копирования в Windows

Периодичность резервного копирования и его тип определяются характером использования компьютера и организационными требованиями. Выполнение резервного копирования может занять достаточно длительное время. Если вы строго придерживаетесь стратегии резервного копирования, то копировать все файлы каждый раз нет необходимости. В этом случае резервное копирование выполняется только для тех файлов, которые были изменены с момента последнего выполнения резервного копирования.

Microsoft Windows включает инструменты резервного копирования, которые можно использовать для резервного копирования файлов. В более ранних версиях, до Windows 8, для резервного копирования файлов использовалась функция Backup and Restore (Архивация и восстановление). Windows 8.1 предлагает функцию File History (История файлов), которая может использоваться для резервного копирования файлов в папках Documents, Music, Pictures, Videos и Desktop. С течением времени эта функция создает историю файлов, позволяя вернуться и восстановить нужную версию какого-либо файла. Это функция, которой удобно пользоваться в случае повреждения или утраты файлов. В Windows 7 и Vista используется другой инструмент резервного копирования, который называется

Backup and Restore (Архивация и восстановление). При выборе внешнего диска Windows 7 предложит использовать его в качестве устройства резервного копирования. Воспользуйтесь функцией архивации и восстановления для управления резервным копированием.

Для доступа к утилите Backup and Restore в Windows 7 выполните следующие шаги

a. Подключите внешний диск.

b. Запустите утилиту Backup and Restore, выполняя следующие шаги.

Start > **Control Panel** > **Backup and Restore (Пуск** > **Панель управления** > **Архивация и восстановление)**

Для доступа к утилите File History в Windows 8,1 выполните следующие шаги

a. Подключите внешний диск.

b. Включите функцию File History (История файлов), выполняя следующие шаги.

Control Panel > **File History** > **Turn on (Панель управления** > **История файлов** > **Включить)**

Примечание. Для других операционных систем также доступны свои инструменты резервного копирования. По умолчанию Apple OS X включает Time Machine, а Ubuntu Linux — Déjà Dup.

Шаг 2: Резервное копирование папок Documents и Pictures

Теперь, когда внешний диск подключен и вы знаете, как найти средство резервного копирования, настройте его так, чтобы резервное копирование папок Documents и Pictures выполнялось каждый день в 3 часа ночи.

a. Откройте **Backup and Restore (Архивация и восстановление)** (Windows 7) или **File History (История файлов)** (Windows 8.x).

b. Выберите внешний диск, на который вы хотите сохранить резервную копию.

c. Укажите, что бы вы хотели скопировать на этот диск. В целях данной лабораторной работы выберите папки **Documents** и **Pictures**.

d. Задайте параметры расписания. В рамках данной лабораторной работы установите «ежедневно, в 3:00».

Почему резервное копирование лучше выполнять в 3:00?

_____

_____

e. Запустите резервное копирование, нажав **Save settings and run backup (Сохранить настройки и начать резервное копирование)**.

Часть 2: Резервное копирование на удаленный диск

Шаг 1: Что такое облачные сервисы резервного копирования

Еще одним вариантом резервного копирования является резервное копирование на удаленный диск. Это может быть полностью облачный сервис или просто сетевое хранилище (NAS), подключенное к сети, в любом случае удаленные резервные копии имеют много общего между собой.

a. Перечислите несколько облачных сервисов резервного копирования.

_____

_____

b. Проанализируйте сервисы, перечисленные выше. Бесплатны ли они?

_____

_____

c. Привязаны ли перечисленные вами сервисы к определенным ОС?

_____

_____

d. Доступны ли ваши данные со всех имеющихся у вас устройств (ПК, ноутбука, планшета и телефона)?

_____

_____

Шаг 2: Использование функции резервного копирования и восстановления для резервного копирования в облако

Выберите сервис, соответствующий вашим потребностям, и выполните резервное копирование папки Documents в облако. Заметим, что сервисы Dropbox и OneDrive позволяют создать папку на компьютере, которую можно будет использовать как ссылку на облачный диск. После того как папка создана, файлы, скопированные в эту папку, автоматически загружаются в облако облачным клиентом, который всегда запущен. Такая настройка очень удобна, так как для планирования облачного резервного копирования можно использовать любые инструменты резервного копирования по вашему выбору. Чтобы воспользоваться функцией Windows Backup and Restore (Архивация и восстановление в Windows) для резервного копирования файлов в Dropbox, выполните шаги ниже.

a. Пройдите по ссылке http://dropbox.com и зарегистрируйте бесплатную учетную запись Dropbox.

b. Когда учетная запись будет создана, Dropbox покажет все файлы, сохраненные в вашей учетной

записи. Нажмите на **свое имя** и щелкните **Install (Установить)**, чтобы загрузить и установить клиент Dropbox, подходящий для вашей операционной системы.

c. Откройте загруженную программу, чтобы установить клиент.

d. После завершения установки клиент Dropbox создаст папку с именем Dropbox внутри папки Home.

Обращаем внимание, что любые файлы, скопированные в эту только что созданную папку, будут автоматически скопированы на серверы, размещенные в облаке Dropbox.

e. Откройте функцию **Windows Backup and Restore (Архивация и восстановление в Windows)** и настройте ее так, чтобы использовать новую папку Dropbox в качестве места назначения резервной копии.

Вопросы для повторения

1. В чем заключаются преимущества резервного копирования данных на локальный внешний диск?

_____

_____

2. В чем заключаются недостатки резервного копирования данных на локальный внешний диск?

_____
_____

3. В чем заключаются преимущества резервного копирования данных на облачный диск?

_____
_____

4. В чем заключаются недостатки резервного копирования данных на облачный диск?

_____

Тема 9. Специалисты в области кибербезопасности
Занятие 9. Поиск вакансий в сфере кибербезопасности

Задачи

Изучение требований к специалистам в сфере кибербезопасности.

Изучение требований к специалистам в сфере кибербезопасности.

Часть 1. Изучение вакансий в сфере кибербезопасности

Часть 2. Требования работодателей к специалистам в сфере кибербезопасности

Общие сведения/сценарий

В кибермире присутствует огромное количество угроз, которые могут представлять опасность как для отдельно взятого человека, так и для организации или государства в целом. Соответственно, существует высокий спрос на специалистов, обладающих знаниями, навыками, профессиональными и моральными качествами, которые необходимы для защиты людей и систем. В ходе этой лабораторной работы вы будете изучать актуальные вакансии и требования к специалистам, а также узнаете, какие документы необходимы для подтверждения квалификации в области кибербезопасности. Существует множество веб-сайтов для поиска вакансий, где можно найти информацию о карьерных возможностях в сфере кибербезопасности. Довольно большую долю в общей массе таких веб-сайтов составляют так называемые агрегаторы вакансий. Агрегаторы собирают объявления о вакансиях, опубликованных множеством других веб-сайтов и организаций. В ходе первой части работы вы изучите три наиболее популярных агрегатора вакансий. Вторая часть будет посвящена изучению требований к специалистам в сфере кибербезопасности.

URL-адрес: http://burning-glass.com/infographic-geography-cybersecurity-jobs-2015/

Необходимые ресурсы

- ПК или мобильное устройство с доступом к Интернету

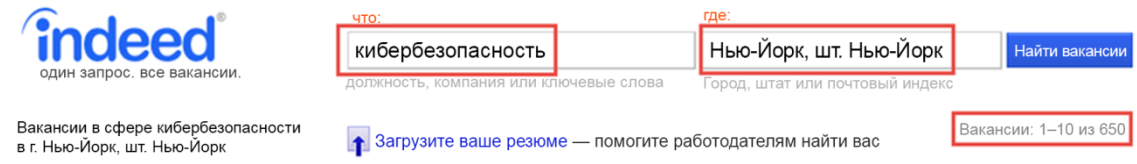
Часть 1: Изучение вакансий в сфере кибербезопасности

Веб-сайт Indeed относится к числу крупнейших агрегаторов вакансий. Услугами Indeed пользуются миллионы соискателей и работодателей. На веб-сайте Indeed публикуется широкий круг вакансий для специалистов любого уровня — от начинающих до руководителей высшего звена. Помимо обычных вакансий, на Indeed можно найти вакансии с частичной занятостью и предложения о прохождении стажировки с последующим трудоустройством.

Шаг 1: Изучение вакансий в сфере кибербезопасности.

d. Откройте браузер и просмотрите видеоролик «Как найти работу на Indeed.com» (https://youtu.be/9gqsnA2Lk-0).

e. Нажмите здесь или перейдите по адресу http://www.indeed.com/, чтобы начать поиск вакансий. Начните с просмотра всех вакансий в г. Нью-Йорк (США). Выполните первый поиск по запросу **cyber security** (кибербезопасность). Запишите количество найденных вакансий.



_____

_____

f. Выполните второй поиск. На этот раз введите запрос **information security** (информационная безопасность). Запишите количество найденных вакансий. По сравнению с предыдущим поиском, в этот раз найдено больше или меньше вакансий? Почему?

_____

_____

g. Введите запрос **network security** (безопасность сети) и выполните поиск в третий раз. Запишите количество найденных вакансий. По сравнению с предыдущим поиском, в этот раз найдено больше или меньше вакансий? Почему?

_____

_____

Шаг 2: Изучение уровня оплаты труда в сфере кибербезопасности

e. Повторите первый поиск вакансий в г. Нью-Йорк (США). Введите запрос **cyber security** (информационная безопасность). Выберите три вакансии. Запишите требования к кандидатам и предлагаемую заработную плату.

_____

_____

_____

_____

f. На веб-сайте Indeed также размещаются вакансии с частичной занятостью и предложения о прохождении стажировки с последующим трудоустройством. Воспользуйтесь функцией **Advanced Job Search** (Расширенный поиск), чтобы найти все предложения о прохождении стажировки по запросу **IT Security** (безопасность ИТ) в г. Нью-Йорк. Сколько предложений выдал веб-сайт? Перечислите несколько заголовков.

_____

_____

g. С помощью функции **Advanced Job Search** (Расширенный поиск) найдите все вакансии с частичной занятостью по запросу **IT Security** (безопасность ИТ) в г. Нью-Йорк. Сколько предложений выдал веб-сайт? Перечислите несколько заголовков.

_____

_____

Часть 2: Требования работодателей к специалистам в сфере кибербезопасности

Для решения задач, связанных с обеспечением кибербезопасности, нужны специалисты высокого класса. Во многих случаях необходимо предоставить дипломы о соответствующем образовании и профессиональные сертификаты, подтверждающие уровень квалификации и знаний. Веб-сайты для поиска вакансий CareerBuilder.com и USAJobs.gov пользуются большой популярностью. На этих веб-сайтах представлены сотни вакансий, связанных со сферой кибербезопасности.

Шаг 1: Изучение веб-сайта CareerBuilder.

a. Нажмите здесь или перейдите по адресу http://www.careerbuilder.com, чтобы начать поиск вакансий с помощью веб-сайта CareerBuilder.com. Начните с просмотра всех вакансий в г. Сан-Франциско, шт. Калифорния (США). Выполните первый поиск по запросу **network security** (безопасность сети). Запишите количество найденных вакансий.

_____

_____

b. Выберите две вакансии, где указана заработная плата. Какая заработная плата предлагается соискателям?

_____

_____

c. Откройте две вакансии, которые вы выбрали на предыдущем шаге. Какие дипломы и сертификаты требуют работодатели? Требуется ли профессиональная сертификация? Перечислите необходимые дипломы об образовании и профессиональные сертификаты.

_____

_____

Шаг 2: Поиск вакансий в государственных учреждениях США.

a. Органы федерального правительства постоянно подвергаются мощным кибератакам. Поэтому многие федеральные ведомства нуждаются в специалистах по кибербезопасности. Нажмите здесь или перейдите по адресу https://youtu.be/f3vRr3Lq-zI, чтобы просмотреть видеоролик о веб-сайте USAjobs.gov. Нажмите здесь или перейдите по адресу https://www.usajobs.gov, чтобы открыть веб-сайт USAJOBS. Выполните поиск, указав название должности **Information Security** (информационная безопасность). Сколько вакансий выдал веб-сайт?

_____

_____

b. Прокрутите содержимое первой страницы с вакансиями и сосчитайте вакансии, опубликованные федеральными ведомствами.

_____

_____

c. Перечислите три заработные платы с первой страницы.

_____

_____

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

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

Методические указания

по организации самостоятельной работы обучающихся
по **дисциплине «ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ»**
для студентов направления подготовки
15.03.05 Конструкторско-технологическое обеспечение
машиностроительных производств
Направленность (профиль) Технология машиностроения

Ставрополь 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ....40
Общая характеристика самостоятельной работы студента 40
Самостоятельное изучение тем лекций....44
Задания по темам учебной дисциплины для самостоятельной работы 45
Задание 1. Идентификация угроз 45
Цели задания 45
Учебные вопросы задания 45
Оборудование и материалы 45
Общие сведения/сценарий 45
Учебный вопрос 1: Настройка FTP-сервера....45
Шаг 1: Активация службы FTP.....45
Шаг 2: Предоставьте пользователям доступ к FTP-серверу.....45
Учебный вопрос 2: Настройка веб-сервера....45
Шаг 1: Активация службы HTTP. 45
Шаг 2: Проверка работоспособности службы HTTP.....45
Учебный вопрос 3: Настройка DNS-сервера....46
Шаг 1: Активация службы DNS. 46
Шаг 2: Создание записей DNS A.....46
Шаг 3: Проверка работоспособности службы DNS.....46
Учебный вопрос 4: Настройка сервера электронной почты....46
Шаг 1: Активация сервисов электронной почты. 46
Шаг 2: Создайте для пользователей учетные записи электронной почты. 46
Шаг 3: Настройка пользовательских клиентов электронной почты. 46
Учебный вопрос 5: Настройка NTP-сервера 47
Шаг 1: Активация службы NTP.....47
Шаг 2: Защита службы NTP.....47
Учебный вопрос 6: Настройка AAA-сервера 47
Шаг 1: Активация службы AAA.....47
Шаг 2: Сетевая конфигурация AAA.....47
Предлагаемый способ подсчета баллов....47
Контрольные вопросы....47
Задание № 2. Общение в кибермире 48
Цели задания 48
Учебные вопросы задания 48
Оборудование и материалы 48
Общие сведения 48
Учебный вопрос 1: Передача электронного сообщения от пользователя к пользователю 48
Шаг 1: Откройте клиент электронной почты на компьютере пользователя Mike. 48
Шаг 2: Отправка электронного сообщения пользователю Sally. 48
Шаг 3: Проверка почты пользователем Sally. 49
Учебный вопрос 2: Загрузка файлов на сервер по протоколу FTP....49
Шаг 1: Настройка анализатора пакетов на перехват трафика соответствующего порта. 49
Шаг 2: Удаленное подключение к FTP-серверу. 49
Шаг 3: Загрузите файл на FTP-сервер.....49
Шаг 4: Анализ FTP-трафика. 49
Учебный вопрос 3: Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet 50
Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети. 50

Учебный вопрос 4: Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH 50
Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети. 50
Предлагаемый способ подсчета баллов 51
Контрольные вопросы 51
Задание № 3. Шифрование файлов и данных 52
Цели задания 52
Учебные вопросы задания 52
Оборудование и материалы 52
Общие сведения 52
Учебный вопрос 1: Поиск данных учетной записи FTP для ноутбука пользователя Mary 52
Шаг 1: Получение доступа к текстовому документу на ноутбуке пользователя Mary... 52
Шаг 2: Расшифровка данных учетной записи FTP пользователя Mary. 52
Учебный вопрос 2: Загрузка конфиденциальных данных на сервер по протоколу FTP ..53
Шаг 1: Просмотр конфиденциального документа на ноутбуке пользователя Mary. ..53
Шаг 2: Удаленное подключение к FTP-серверу. 53
Шаг 3: Загрузите файл на FTP-сервер. 53
Учебный вопрос 3: Поиск данных учетной записи FTP для компьютера пользователя Bob 53
Шаг 1: Получение доступа к текстовому документу на компьютере пользователя Bob. 53
Шаг 2: Расшифровка данных учетной записи FTP пользователя Bob. 53
Учебный вопрос 4: Загрузка конфиденциальных данных с сервера по протоколу FTP ..54
Шаг 1: Удаленное подключение к FTP-серверу. 54
Шаг 2: Загрузите файл на компьютер пользователя Bob. 54
Учебный вопрос 5: Расшифровка содержимого файла clientinfo.txt 54
Шаг 1: Получение ключа расшифровки от пользователя Mary. 54
Шаг 2: Расшифровка содержимого файла clientinfo.txt. 54
Предлагаемый способ подсчета баллов 55
Контрольные вопросы 55
Задание № 4. Проверка целостности файлов и данных 56
Цели задания 56
Учебные вопросы задания 56
Оборудование и материалы 56
Общие сведения 56
Учебный вопрос 1: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike 56
Шаг 1: Получение доступа к FTP-серверу с компьютера пользователя Mike. 56
Шаг 2: Файловый сервер взломан. Об этом необходимо уведомить пользователя Sally. 57
Учебный вопрос 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File 57
Шаг 1: Получение доступа к внешнему FTP-серверу с компьютера пользователя Mike. 57
Шаг 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike. 57
Учебный вопрос 3: Проверка целостности файлов с информацией о клиентах с помощью хеширования 58
Шаг 1: Проверка хеш-сумм на компьютере пользователя Mike. 58
Шаг 2: Загрузка подозрительного файла на компьютер пользователя Sally. 58

Учебный вопрос 4: Проверка целостности критически важных файлов с помощью механизма HMAC 58
Шаг 1: Расчет HMAC-суммы критически важного файла. 58
Шаг 2: Проверьте полученную HMAC-сумму. 59
Предлагаемый способ подсчета баллов 59
Контрольные вопросы 59
Задание № 5. WEP/WPA2 PSK/WPA2 RADIUS 61
Цели задания 61
Учебные вопросы задания 61
Оборудование и материалы 61
Общие сведения 61
Учебный вопрос 1: Настройка WEP на объекте Healthcare at Home 61
Шаг 1: Настройка идентификатора SSID беспроводной сети. 61
Шаг 2: Настройка защиты беспроводной сети. 62
Шаг 3: Подключение клиентских устройств. 62
Учебный вопрос 2: Настройка WPA2 PSK на объекте Gotham Healthcare Branch 62
Шаг 1: Настройка идентификатора SSID беспроводной сети. 62
Шаг 2: Настройка защиты беспроводной сети. 62
Шаг 3: Подключение клиентских устройств. 62
Учебный вопрос 3: Настройка WPA2 RADIUS на объекте Metropolis Bank HQ 63
Шаг 1: Настройка идентификатора SSID беспроводной сети. 63
Шаг 2: Настройка защиты беспроводной сети. 63
Шаг 3: Настройка сервера RADIUS. 63
Шаг 4: Подключение клиентских устройств. 63
Предлагаемый способ подсчета баллов 64
Контрольные вопросы 64
Задание № 6. Настройка транспортного режима VPN 65
Цели задания 65
Учебные вопросы задания 65
Оборудование и материалы 65
Общие сведения 65
Учебный вопрос 1: Передача незашифрованного FTP-трафика 65
Шаг 1: Получение доступа к анализатору трафика Cyber Criminals Sniffer. 65
Шаг 2: Установите небезопасное FTP-соединение с сервером Public_FTP. 65
Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer. 66
Учебный вопрос 2: Настройка VPN-клиента на компьютере пользователя Phil 66
Учебный вопрос 3: Передача зашифрованного FTP-трафика 66
Шаг 1: Просмотр текущих параметров IP-адресации на компьютере пользователя Phil. 66
Шаг 2: Передача зашифрованного FTP-трафика с компьютера пользователя Phil на сервер Private_FTP. 66
Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer 67
Предлагаемый способ подсчета баллов 67
Контрольные вопросы 67
Задание № 7. Настройка туннельного режима VPN 68
Цели задания 68
Учебные вопросы задания 68
Оборудование и материалы 68
Общие сведения 68
Учебный вопрос 1: Передача незашифрованного FTP-трафика 68

Шаг 1: Получение доступа к анализатору трафика Cyber Criminals Sniffer. 68
Шаг 2: Установка небезопасного FTP-соединения с резервным FTP-сервером. 68
Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer. 69
Учебный вопрос 2: Настройка VPN-туннеля между объектами Metropolis и Gotham 69
Учебный вопрос 3: Передача зашифрованного FTP-трафика 69
Шаг 1: Отправка FTP-трафика с компьютера пользователя Sally на резервный файловый сервер File Backup. 69
Шаг 2: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer 70
Предлагаемый способ подсчета баллов 70
Контрольные вопросы 70
Задание № 8. Резервирование маршрутизаторов и коммутаторов 71
Цели задания 71
Учебные вопросы задания 71
Оборудование и материалы 71
Общие сведения 71
Учебный вопрос 1: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов. 71
Шаг 1: Откройте командную строку на компьютере пользователя Phil. 71
Шаг 2: Проследите маршрут к внешнему веб-серверу. 71
Шаг 3: Запустите переключение при отказе сетевой инфраструктуры. 72
Шаг 4: Снова проследите маршрут к внешнему веб-серверу. 72
Учебный вопрос 2: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов. 72
Шаг 1: Откройте командную строку на компьютере Tim's. 72
Шаг 2: Проследите маршрут к внешнему веб-серверу. 72
Шаг 3: Запустите переключение при отказе сетевой инфраструктуры. 73
Шаг 4: Снова проследите маршрут к внешнему веб-серверу. 73
Предлагаемый способ подсчета баллов 74
Контрольные вопросы 74
Задание № 9. Резервирование маршрутизаторов и коммутаторов 75
Цели задания 75
Учебные вопросы задания 75
Оборудование и материалы 75
Общие сведения 75
Учебный вопрос 1: Повышение надежности конфигурации IOS 75
Шаг 1: Откройте командную строку на компьютере Sally's. 75
Шаг 2: Выполните удаленное подключение к маршрутизатору HQ_Router. 75
Шаг 3: Создайте правовое уведомление на маршрутизаторе HQ_Router. 75
Шаг 4: Включите защиту паролем на маршрутизаторе HQ_Router. 76
Учебный вопрос 2: Активация функции Cisco IOS Resilient Configuration 76
Шаг 1: Просмотрите текущий образ IOS. 76
Шаг 2: Обеспечьте защиту текущего образа и конфигурации. 76
Предлагаемый способ подсчета баллов 77
Контрольные вопросы 77
Задание № 10. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе 78
Цели задания 78
Учебные вопросы задания 78
Оборудование и материалы 78
Общие сведения 78

Учебный вопрос 1: Подключение к веб-серверу. 78
Шаг 1: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP. 78
Шаг 2: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS. 78
Учебный вопрос 2: Запрет незашифрованных сеансов HTTP. 79
Шаг 1: Настройте маршрутизатор HQ_Router. 79
Шаг 2: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP. 79
Шаг 3: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS. 79
Учебный вопрос 3: Доступ к межсетевому экрану на сервере электронной почты. 79
Предлагаемый способ подсчета баллов 80
Контрольные вопросы 80
Задание № 11. Отработка комплексных практических навыков 81
Цели задания 81
Оборудование и материалы 81
Сценарий 81
Реализация 81
Предлагаемый способ подсчета баллов 82

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.

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

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим 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, форму-

лировки, 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;

– подготовка к практическим заданиям, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображение структуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы;

3) для формирования умений:

– подготовка к практическим 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 зада-

ния, 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, отвечаю-

щей 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 специалистов 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

Учебный вопрос 1: Настройка FTP-сервера

Шаг 1: Активация службы FTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.

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

c. Включите службу FTP с помощью селективной кнопки, которая находится в верхней части окна.

Шаг 2: Предоставьте пользователям доступ к FTP-серверу.

a. Создайте учетные записи пользователей с именами **bob**, **mary** и **mike**, назначив каждой из них пароль **cisco123**.

b. Каждая учетная запись должна иметь полные разрешения (RWDNL) на доступ к серверу FTP/Web.

Учебный вопрос 2: Настройка веб-сервера

Шаг 1: Активация службы HTTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.

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

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

Шаг 2: Проверка работоспособности службы HTTP.

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

b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.

c. Пользуясь веб-браузером, перейдите по IP-адресу **10.44.1.254**.

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

_____

_____

Учебный вопрос 3: Настройка DNS-сервера

Шаг 1: Активация службы DNS.

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

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

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

Шаг 2: Создание записей DNS A.

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

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

Шаг 3: Проверка работоспособности службы DNS.

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

b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.

Почему пользователь успешно переходит по указанному полностью квалифицированному имени домена?

_____

_____

Учебный вопрос 4: Настройка сервера электронной почты

Шаг 1: Активация сервисов электронной почты.

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

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

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

Шаг 2: Создайте для пользователей учетные записи электронной почты.

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

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

Шаг 3: Настройка пользовательских клиентов электронной почты.

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

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

Name (Имя): **Sally**

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

Incoming & 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?

_____

_____

Учебный вопрос 5: Настройка NTP-сервера

Шаг 1: Активация службы NTP.

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

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

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

Шаг 2: Защита службы NTP.

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

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

Учебный вопрос 6: Настройка AAA-сервера

Шаг 1: Активация службы AAA.

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

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

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

Шаг 2: Сетевая конфигурация AAA.

a. Введите имя Client Name (имя клиента) **HQ_Router**, адрес Client IP (IP-адрес клиента) **10.44.1.1** и пароль **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить параметры клиента.

b. Настройте учетную запись пользователя AAA **admin** с паролем **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить информацию о пользователе.

Предлагаемый способ подсчета баллов

Вопросы 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 **OK**.

e. Полностью скопируйте содержимое текстового документа.

f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://www.tools4noobs.com/online_tools/hash/.

g. Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Убедитесь в том, что выбран алгоритм md2. Нажмите кнопку **Hash this!** (Вычислить хеш-сумму).

h. Чтобы удостовериться в том, что содержимое файла не было искажено, сравните полученную хеш-сумму с соответствующей хеш-суммой из списка файлов, который вы получили на шаге 1 в части 2.

i. Повторите шаги d–h для каждого файла с информацией о клиентах и сравните полученные хеш-суммы с первоначальными хеш-суммами из списка файлов, который вы получили на шаге 1 в части 2.

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

_____

Шаг 2: Загрузка подозрительного файла на компьютер пользователя Sally.

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

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

c. Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.

d. Введите имя пользователя **sally** и пароль **cisco123**.

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

f. Загрузите с сервера искаженный файл, выявленный на шаге 1 в части 3.

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

h. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы удостовериться в том, что искаженный файл успешно загружен на компьютер пользователя Sally для последующего анализа.

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

Шаг 1: Расчет HMAC-суммы критически важного файла.

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

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

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

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

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

f. Выберите документ **income.txt** и нажмите кнопку **OK**.

g. Полностью скопируйте содержимое текстового документа.

h. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт http://www.freeformatter.com/hmac-generator.html.

i. Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Введите секретный ключ **cisco123**. Убедитесь в том, что выбран алгоритм **SHA1**. Нажмите кнопку **Compute HMAC** (Рассчитать HMAC).

Какова HMAC-сумма содержимого файла?

_____

Почему механизм HMAC безопаснее обычного хеширования?

_____

Шаг 2: Проверьте полученную HMAC-сумму.

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

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).

d. Перейдите по ссылке, чтобы просмотреть список новейших файлов и соответствующих хеш-сумм.

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

_____

Предлагаемый способ подсчета баллов

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

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	Интер-фейс	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