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 специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

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/cybersecurityessentials-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? Приведите примеры

_____

_____

Изучение недавних атак.

a. Последствия и масштаб недавних кибератак обеспокоили многих руководителей в частных и государственных структурах. Нажмите https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/ чтобы прочесть о десяти наиболее разрушительных угрозах 2022 г.

Приведите примеры.

_____

_____

b. Опишите кибератаки (10 примеров), совершенные за 2022 год, по схеме: 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 пароль,

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 онлайнсервисов 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/april 12/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/serverstorage/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 интернетподключения.

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 1: 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-passwordgenerator/.
e. Создайте случайный словарный пароль, нажав кнопку **Generate Another! (Создать другой!)** вверху веб-страницы.
f. Легко ли запомнить созданный пароль?

_____

_____

Часть 2: 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 3: 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 (ЛЮБОЕ, например Dropbox)

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

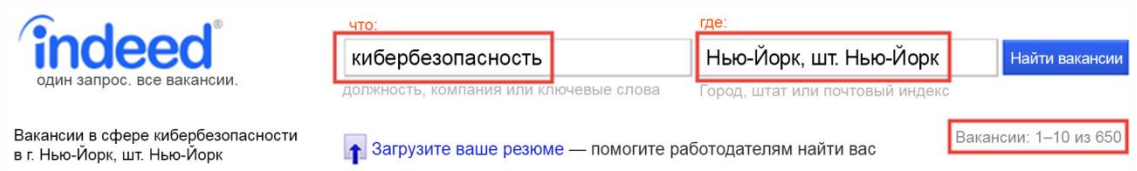
Часть 1: **Изучение вакансий в сфере кибербезопасности**

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.

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.

Список рекомендуемой литературы

Перечень основной литературы:

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс Электронный ресурс: учебное пособие / М.Ю. Щербаков / Н.И. Синадский / А.С. Коллеров / А.Н. Андрончик; ред. Н.И. Синадский. – Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс,2022-08-31. - Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2014. – 180 с. – Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7996-1201-6

Перечень дополнительной литературы:

1. Осипенко А.Л. Сетевая компьютерная преступность. Теория и практика борьбы Электронный ресурс: Монография / А.Л. Осипенко. – Омск: Омская академия МВД России, 2009. – 480 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 978-5-88651-445-2

2. Тишина Н.А. Прикладные задачи безопасности информационно-телекоммуникационных систем Электронный ресурс: Учебное пособие / Н.А. Тишина, Е.Н. Чернопрудова. – Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. – 122 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 978-5-7410-1892-7

3. Филиппов Б.И. Информационная безопасность. Основы надежности средств связи Электронный ресурс: Учебник / Б.И. Филиппов, О.Г. Шерстнева. – Саратов: Ай Пи Эр Медиа, 2019. – 227 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4486-0485-0

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

Методические указания для студентов по организации самостоятельной работы по дисциплине "Персональная кибербезопасность": Специальность 10.05.01 Компьютерная безопасность; Квалификация выпускника – специалист по защите информации; Форма обучения - очная; Учебный план 2021 г. - Ставрополь, 2021.

Методические указания по выполнению лабораторных работ по дисциплине "Персональная кибербезопасность": Специальность 10.05.01 Компьютерная безопасность; Квалификация выпускника – специалист по защите информации; Форма обучения – очная; Учебный план 2021 г. – Ставрополь, 2021.

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