Публичные сети Wi-Fi

Этот урок посвящен преимуществам и рискам публичных сетей Wi-Fi. Расскажите учащимся, как определить незащищенную сеть Wi-Fi, чем опасны такие сети и в каких случаях их можно использовать.

Ресурсы

- Изображение беспроводного модема
- Раздаточный материал по теме "Безопасное подключение к Интернету"

Что такое Wi-Fi?

Часть первая

Вопросы ученикам

С каких устройств вы выходите в Интернет?

Как эти устройства подключаются к Интернету?

Схема взаимодействия в группе

Для подключения устройств к Интернету люди часто используют Wi-Fi. Wi-Fi — это беспроводная сеть, которая обеспечивает подключение устройств к Интернету с помощью радиосигнала.

Представьте себе, что у вас дома три ноутбука и вы хотите подключить их к Интернету. Для этого вам понадобится следующее:

1. Точка доступа. Это любое устройство, которое отправляет сигналы Wi-Fi для подключения к Интернету. Чтобы подключиться к Интернету, ваши устройства должны принять эти сигналы. Иногда для использования точки доступа необходимо сначала получить разрешение (например, имя пользователя и пароль).

2. Маршрутизатор. Это устройство, которое объединяет в единую сеть все электронные устройства, например компьютеры, планшеты и мобильные телефоны, находящиеся в определенном месте (в школе, библиотеке, дома и т. д.). Как правило, в маршрутизатор встроена точка доступа (см. схему выше).

> Зона действия маршрутизатора ограничена (как правило, она очень мала). Чем дальше вы от маршрутизатора, тем слабее сигнал Wi-Fi. Кроме того, сигналы маршрутизатора может ослабить здание, кирпичная стена и другие объекты, которые находятся между маршрутизатором и вами.
>
> Через маршрутизатор можно подключиться к сети, которую он создал, но не к Интернету. Чтобы затем вы могли подключиться к Интернету, маршрутизатор нужно подключить к модему.

3. Модем. Это устройство, которое устанавливает и поддерживает подключение к интернет-провайдеру. Модем преобразует внешние сигналы в сигналы, которые может считать ваш компьютер и другие электронные устройства.

> Обычно точка доступа и маршрутизатор — это одно и то же устройство,

физически подключенное к модему по специальному кабелю — Ethernet. Такое подключение называют "проводным".

Мобильное устройство также может подключаться к Интернету по мобильной связи, особенно когда другие способы подключения недоступны. Зона действия мобильной связи гораздо шире, чем зона действия маршрутизатора. Ее формируют вышки мобильной связи — станции, которые передают и принимают специальные радиосигналы.

Часть вторая

Вопросы ученикам

Какие преимущества предлагает Wi-Fi?

А недостатки?

Почему сети Wi-Fi менее защищены, чем проводные сети?

Почему на улице ваш телефон не может подключиться к Wi-Fi?

Выбор сети Wi-Fi

Часть первая

Вопросы ученикам

Все ли сети Wi-Fi защищены? Почему?

Текст для преподавателя

Иногда у вас есть сразу несколько сетей Wi-Fi, и вам необходимо выбрать, к какой из них подключаться. Помните, что подключаться к незащищенным сетям Wi-Fi очень опасно. Незащищенные сети Wi-Fi — это сети, которые доступны без пароля. В них информацию, которую вы передаете, могут видеть другие пользователи. Это позволяет им следить за вами или красть ваши данные.

В защищенных сетях Wi-Fi для доступа необходим пароль, а также используется шифрование. Однако иногда злоумышленники пытаются выдать незащищенные сети за защищенные. Для этого они дают им названия, похожие на названия защищенных сетей (например, вашей школьной сети). Доверять следует только тем сетям, которые используют максимум средств защиты.

Обращайте внимание на то, где или в каких условиях вы подключаетесь к сети Wi-Fi. Например, школьная сеть Wi-Fi не может быть доступна за пределами школы. Если ваше устройство "найдет" сеть с похожим названием в кинотеатре, будьте уверены, что это подделка, с помощью которой злоумышленники пытаются выкрасть у школьников пароли.

При настройке защищенной паролем сети Wi-Fi ее владелец должен включить на маршрутизаторе протокол шифрования. Чаще всего используются протоколы шифрования WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) или WPA2. Они шифруют информацию, передаваемую по сети.

Это затрудняет хакерам перехват информации, передаваемой по такой сети. Тем не менее любой из этих протоколов (WEP, WPA и WPA2) можно взломать. Поэтому при передаче информации онлайн также необходимо безопасное веб-подключение.

Для шифрования передаваемых через Интернет данных сайты используют стандарт HTTPS. Он защищает ваши данные от перехвата. Чтобы воспользоваться им, достаточно в любом браузере перед любым URL ввести "https://" (например, https://www.mysite.com). Однако не все сайты поддерживают HTTPS.

1. На веб-страницах без префикса HTTPS:// не следует вводить конфиденциальную информацию (пароли, данные кредитных карт и т. д.).

2. В большинстве браузеров на соединение HTTPS указывает значок замка рядом с адресной строкой.

3. К сожалению, HTTPS защищает ваши данные только в момент передачи на сайт, но не гарантирует, что затем они не попадут "не в те руки". Кроме того, этот стандарт могут использовать и вредоносные сайты.

Текст для преподавателя

Протокол SSL или TLS — это технология, позволяющая обеспечить безопасное подключение по стандарту HTTPS. SSL или TLS использует цифровые ключи шифрования — примерно то же самое, что и обычные ключи. Например, если вы отправите другу записку, ее сможет прочитать любой, кому она попадет в руки. Однако вы можете обмениваться записками в парных коробках, ключи от которых есть только у вас и у друга. Если кто-то перехватит вашу корреспонденцию, ему будет непросто открыть коробку без ключа. Кроме того, если злоумышленник подменит коробку, вы не сможете открыть ее имеющимся ключом и сразу же заподозрите неладное. SSL или TLS работает по тому же принципу.

Индикаторы безопасности браузера также передают расширенный сертификат подлинности EV (Extended Validation). Сертификаты EV получают сайты, которые одобрены контролирующим органом. Иногда в браузерах индикатор EV отображается в виде названия сайта или регистрирующего органа рядом с адресной строкой. Если вы сомневаетесь в том или ином сайте, посмотрите, совпадает ли URL в сертификате с URL в браузере — для этого нажмите View Certificate (Посмотреть сертификат). Чтобы учащимся было понятнее, на экране проектора покажите, где находится эта кнопка. В разных браузерах эта кнопка может находиться в разных местах. Например, в браузере Chrome откройте меню View (Вид), нажмите Developer (Разработчик), а затем Developer Tools (Инструменты разработчика). В разделе Developer Tools (Инструменты разработчика) выберите вкладку Security (Безопасность) и нажмите View Certificate (Посмотреть сертификат).

Вопросы ученикам

Что нужно учитывать при подключении к новой сети?

1. Возможные варианты ответа: местоположение (или владелец сети), уровень доступа (кто ещё может подключиться к сети) и задачи пользователя (что он намерен делать в сети).

Кому принадлежит сеть Wi-Fi у вас дома? В школе? В кафе?

1. Ваша домашняя сеть принадлежит вашим родителям или опекунам, школьная — администрации школы или района, а сеть в кафе — его владельцу.

Знаете ли вы этих людей лично? Доверяете ли вы им?

1. Предложите учащимся обсудить, насколько они доверяют каждому из этих лиц.

Текст для преподавателя

Сеть Wi-Fi можно считать надежной, только если вы знаете ее владельца и доверяете ему. Иногда владельца сети можно определить по ее SSID.

Идентификатор SSID (Service Set Identifier) — это название сети Wi-Fi, которое вы видите, когда пытаетесь к ней подключиться. Как правило, по SSID можно не только определить владельца, но и получить другие сведения о сети. Однако не забывайте, что SSID можно выбирать произвольно — достаточно знать, как это делается. Например, злоумышленники могут задать для своей сети такой же SSID, как у вашей школьной сети. Эта хитрость помогает им выведать имена пользователей и пароли учащихся.

Зная владельца сети, проще понять, защищена ли она. Если сеть принадлежит человеку или организации, которым вы доверяете, к ней можно смело подключаться. К неизвестной сети подключаться не стоит — кто знает, кому принадлежит ее маршрутизатор? Помните, что владелец маршрутизатора может отслеживать или записывать весь трафик, который через него проходит.

При использовании Wi-Fi ваше устройство подключается к Интернету через локальную сеть устройств. Вы должны доверять всем устройствам в этой сети, поскольку вам придется обмениваться с ними данными. Это как работа в группе — если ее участники не доверяют друг другу, ничего не получится!

Ограничить доступ к сети помогает пароль. Даже если сеть с паролем находится в общественном месте (например, в кафе), доступ к ней можно контролировать — в отличие от полностью открытых сетей.

Прежде чем подключаться к подозрительной сети, подумайте, действительно ли это вам необходимо, и тщательно взвесьте риски. Например, подумайте, стоит ли ради сиюминутного удобства рисковать безопасностью своего аккаунта?

Вопросы ученикам

Стоит ли читать новости онлайн или блоги по сети Wi-Fi дома? В школе? В

кафе?

1. На веб-странице обычно не содержится конфиденциальной информации. Поэтому в данном случае вам подойдет практически любая сеть.

Стоит ли отправлять номер кредитной карты по сети Wi-Fi у вас дома? В школе? В кафе? Почему?

1. Обсудите с учащимися, почему домашняя сеть Wi-Fi подходит для этого гораздо лучше, чем Wi-Fi в кафе. Объясните, что такой информацией нельзя делиться даже в надежной школьной сети, поскольку она строго конфиденциальна.

Стоит ли проверять электронную почту по Wi-Fi дома? В школе? В кафе?

1. Объясните, что домашняя сеть в этом случае наиболее безопасна. Также скажите, что уровень конфиденциальности электронного письма зависит от его содержания. Например, у некоторых людей сразу несколько аккаунтов, которые они используют с разными целями (один для рекламы, второй для переписки с друзьями и родственниками и т. д.).

Текст для преподавателя

Пароли, банковские реквизиты и другую конфиденциальную информацию лучше отправлять и просматривать в защищенной конфиденциальной сети на сайтах, где используется SSL или TLS. В публичной сети, к которой может подключиться кто угодно, делать это небезопасно.

Уровень конфиденциальности информации зависит в том числе от того, как к ней относится владелец. В конечном итоге решение остается за вами. Прежде чем подключиться, спросите себя, доверяете ли вы владельцу сети, другим ее пользователям, что вы собираетесь делать и какой информацией вы будете делиться онлайн.

Защищенные и незащищенные сети

Часть первая

Взаимодействие в группе

Внимание! Некоторые темы этого занятия уже обсуждались на уроке 2: "Выбор сети Wi-Fi". Вы можете повторить или пропустить их.

Текст для преподавателя

Как вам известно, незащищенные сети Wi-Fi — это сети, для доступа к которым не нужен пароль. В таких сетях передавать и принимать данные опасно.

В безопасных сетях Wi-Fi используется шифрование и пароль для доступа. Шифрование включает человек, который настраивает сеть. Если шифрование включено, передаваемая по сети информация кодируется, благодаря чему хакеру гораздо сложнее ее перехватить.

Однако если сеть защищена, это ещё не значит, что ваши данные в полной безопасности. Хотя защищенная сеть в любом случае лучше незащищенной, в ней вашу информацию тоже могут похитить.

Три самых распространенных протокола шифрования в сетях Wi-Fi: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) и WPA2. Протоколы WEP и WPA устарели, поэтому сети, где они используются, считаются незащищенными. Однако и протокол WPA2 можно взломать.

Чтобы защитить свою информацию, пользуйтесь только сайтами, на которых включено шифрование SSL или TLS.

Вопросы ученикам

Приведите пример защищенной паролем сети, которой вы пользуетесь.

1. Это может быть сеть Wi-Fi у вас дома, в школе и в некоторых общественных местах (например, в кафе).

Приведите пример незащищенной сети, которой вы пользуетесь.

Какие примеры защищенных сетей вы можете привести?

Текст для преподавателя

Чтобы узнать, шифруются ли данные в сети Wi-Fi, проверьте настройки сети

или беспроводного подключения на своем устройстве.

Часть вторая

Взаимодействие в группе

Перед занятием найдите в Интернете информацию о том, как проверить типы шифрования в сетях Wi-Fi в разных операционных системах. Затем продемонстрируйте этот процесс учащимся. Например, в MacOS выберите System Preferences (Предпочтения системы) -> Network (Сеть) -> Wi-Fi и название нужной вам сети. Во вкладке Wi-Fi отобразится список обнаруженных сетей с типами шифрования в отдельном столбце.

Текст для преподавателя

Не все подключения одинаковы. К незащищенной сети может подключиться кто угодно, и неясно, кто ею управляет. В такой сети ваш веб-трафик (страницы, пароли и т. д.) уязвим — теоретически его может просмотреть любой другой пользователь сети, если на сайте, которым вы пользуетесь, не применяется технология SSL или TLS.

Взаимодействие в группе

Если уровень технических знаний учащихся позволяет, вы можете рассказать им, как обеспечить дополнительную защиту сети Wi-Fi с помощью виртуальной частной сети (VPN). Подробнее о технологии VPN см. в разделе "Ресурсы".

Безопасное подключение к Интернету

Название части

Взаимодействие в группе

Разбейте участников на группы по 2–3 человека. Раздайте материалы к уроку "Безопасное подключение к Интернету" и предложите каждой группе свой сценарий. Дайте участникам на обсуждение 5 минут. После этого попросите участников озвучить свои ответы. В раздаточных материалах ответы выделены зеленым.

Задание

Часть первая

Задание

Попросите учащихся:

1. Рассказать, какими сетями Wi-Fi они пользуются в разное время суток.

2. Кратко рассказать о двух таких сетях. Например, кто ещё ими пользуется, насколько они защищены и т. д.

3. Объяснить, для чего можно использовать эти сети и какие риски они создают.