ЗАЩИТА ИНФОРМАЦИИ на мобильных устройствах

Галина Николаевна Климонтова, *заместитель директора средней школы № 3 г. Лебедянь Липецкой области*

Технологии беспроводной передачи данных активно развиваются. Свободное передвижение пользователя и потребность в быстром доступе в Интернет — это и есть главный стимул их развития. Сегодня для беспроводного доступа в Интернет используются различные технологии: Wi-Fi, WiMAX, GPRS/EDGE, спутниковые каналы связи и т.п. Все эти технологии доступны через мобильные устройства. Каждое следующее поколение мобильных устройств становится сложнее, приобретая возможности компьютеров, что также увеличивает угрозы, которым они подвержены.

• *узел сети* • *пользователи мобильных устройств* • *уровень опасности* • *уровень защищённости* • *защита информации* • *мобильные приложения*

Какие же устройства на самом деле мобильные и почему их так называют? Прежде мобильным называли любое устройство для телефонной связи, которое можно носить с собой. Теперь в нашем распоряжении смартфоны, планшеты, электронные книги и прочие «гаджеты», которые сопровождают нас повсюду и без которых мы не мыслим своего существования. При этом помимо телефонной связи они поддерживают множество других функций. Таким образом, мобильные устройства перестали быть *телефонами*. Они превратились в мобильные компьютеры, книги, развлекательные панели, игровые консоли и точки доступа к социальным сетям.

В разных источниках мы нашли несколько понятий:

Мобильное устройство:

• (англ. *Mobile Internet Device, MID*) — компактные мобильные компьютеры с размером диагонали экрана 4–7 дюймов (10–17,8 см), предназначенные прежде всего для просмотра веб-страниц и работы с веб-сервисами, развлечения и коммуникации [5].

• наладонные или карманные компьютеры (КПК), сотовые телефоны, видеокамеры, цифровые фотоаппараты и другие системы, которые объединяют все перечисленные функции [6].

• девайс, который соответствует таким характеристикам: портативный, персональный, он почти всё время с тобой, им можно легко и быстро пользоваться, у него есть какое-нибудь подключение к Интернету [4].

Российский рынок планшетных компьютеров в 2013 году вырос на 108% по сравнению с 2012 годом, до 8,58 миллиона устройств. По прогнозу IDC, неумолимое наступление мобильных устройств продолжится: продажи планшетов возрастут на 18%, смартфонов — на 12%. В 2015 году ёмкость рынка планшетов превзойдёт совокупное количество продаваемых ноутбуков и настольных компьютеров [3].

Что же такое сегодня мобильное устройство с точки зрения защиты информации? —
Более чем полноценный узел Сети:
• больше сетевых интерфейсов, всегда онлайн;
• синхронизация с «большими» ПК;
• «Деньги на борту» (сотовый оператор, ДБО, магазины приложений);
• авторизация в интернет-сервисах и т.д.

Менее защищённый узел сети:
• непрозрачные процессы и содержимое файловой системы;
• доступность интерфейсов съема информации;
• отсутствие цифровой гигиены и халатное отношение и т.д.

Анализируя выводы экспертов IDC, мы видим, что значительная часть повседневной активности пользователей вроде навигации по сайтам и просмотру почты переносится на компактные мобильные устройства, которые отличаются продолжительным временем автономной работы.

Пользователи

Самые активные пользователи мобильных устройств — дети, подростки и молодёжь. По данным Всероссийского центра изучения общественного мнения (ВЦИОМ), в России ежедневно пользуются Интернетом 89% подростков в возрасте 12–17 лет, что вместе с детьми до 12 лет составляет ещё около 10 млн пользователей [3].

Основная потребность школьников при использовании планшетного компьютера — быстрый доступ в социальные сети, электронной почте, к сетевым играм, что не всегда безопасно. Несмотря на популярность мобильных устройств, среди пользователей-школьников, в школьной программе по предмету «Информатика и ИКТ» вопросы безопасного использования мобильных устройств и защиты информации не рассматриваются.
И сегодня этот вопрос стоит остро как перед разработчиками современных устройств, так и перед педагогической и родительской общественностью.

Уровень защищённости

Мобильные устройства более уязвимы по сравнению с обычными персональными компьютерами, так как для выхода в Интернет они используют публичные сети, а встроенные средства защиты не всегда способны обеспечить требуемый уровень защищённости, например, в ОС *Android* отсутствует встроенный сетевой экран; отсутствуют поддержка российских алгоритмов шифрования и сертификаты соответствия требованиям ФСБ РФ и ФСТЭК РФ, что не позволяет использовать мобильные устройства при подключении к корпоративным сетям государственных органов и учреждений.

По результатам исследования нарушений пользовательской приватности в популярных приложениях для Android, аналитики известной антивирусной компании BitDefender обнаружили, что около 13% приложений собирают и передают «на сторону» номера мобильных телефонов пользователей без уведомления. Приблизительно столько же передают данные о местонахождении владельца, почти 8% собирают адреса электронной почты, почти 6% получают доступ к журналу браузера, а некоторые даже к личным фотографиям [8].

Компания Bit9, занимающаяся вопросами информационной безопасности, отмечает, что более 100 000 приложений Android, размещённых в Google Play, считаются «сомнительными»: 42% приложений получают GPS-данные о местоположении пользователя; 31% получают сведения о номере телефона или звонках; 26% имеют доступ к личным данным (контакты и электронная почта); 9% используют функции, которые могут стоить пользователю денег [7].

По данным Symantec за 2013 год, в среднем каждый месяц появлялось 5 новых типов и 272 разновидности вредоносных программ, цель которых — устройства на платформе Android [1]. Угрозы разно-

образны: кража личных данных и финансовой информации, слежка за пользователями, отправка с их устройств платных sms-сообщений, отображение назойливой рекламы и множество других.

Специалисты ОАО «Инфотекс» (г. Москва) наблюдали за трафиком, оставленным на сутки на подзарядке и подключённым к Интернету iPada. Было установлено, что кроме защищённого обмена информацией были IP-адреса, с которыми iPad организовал общение без ведома пользователя.

Вредоносные программы для Android, как правило, устанавливаются пользователем через магазины приложений. Однако всё более тщательная проверка администрацией магазинов приложений на предмет вредоносного кода делает размещение вирусописателями своих программ всё более трудным. Вместо этого злоумышленники начинают использовать стационарные компьютеры как способ доставки вредоносного ПО на Android-устройства. Это приводит к появлению гибридных угроз.

Информация на мобильном устройстве, которая может заинтересовать злоумышленников

Содержание переписки в электронной почте. Чаще всего пользователи сохраняют учётные данные своих аккаунтов в настройках клиента. Получив доступ к устройству, злоумышленники имеют возможность просматривать всю переписку, а также иметь доступ к сервисам, привязанным к данному почтовому ящику.

Интернет-пейджеры. Skype, Icq, социальные сети доступны современным мобильным устройствам, в результате чего вся переписка конкретного человека и его контакт-листы могут быть под угрозой.

Документы, файлы. Мобильные устройства имеют достаточно большой объём памяти. Хранимая на личных мобильных устройствах информация может быть интересна злоумышленникам.

Адресная книга. Адреса электронной почты традиционно представляют интерес для спамеров и приложений, рассылающих вирусы.

Средства удалённого доступа. Использование смартфона или планшета для удалённого доступа к рабочему месту с помощью средств удалённого администрирования уже не редкость для современного пользователя.

Мобильный банкинг. Частные мобильные платежи получили широкое распространение в последние годы. Крупные суммы с помощью мобильного банкинга у подростка перевести, может быть и не удастся, а вот украсть несколько тысяч рублей через планшет злоумышленникам вполне под силу.

Уровни опасности

Как видим, современные мобильные устройства нуждаются в сильных мерах защиты, а имеющиеся встроенные средства защиты не всегда способны обеспечить требуемый уровень защищённости. Однако их применение не должно быть в ущерб удобству.

В сложившейся ситуации большинство пользователей (взрослые, дети, подростки) мобильных устройств не знают об грозящих опасностях и пользуются мобильными устройствами при отсутствии на них средств защиты. Тем не менее подрастающее поколение, имеющее в кармане иногда даже не по одному современному гаджету, должно понимать уровень грозящей опасности и уметь предотвратить возможный вред. Здесь задачу образования в области защиты информации на мобильных устройствах должны решать образовательные организации.

Защита информации

При составлении рабочей программы по предмету «Информатика и ИКТ» в нашей школе обязательной частью учебного материала главы «Компьютер как средство автоматизации информационных процессов» в 11-м классе стали

темы организации защиты информации на мобильных устройствах, которая не предусмотрена для изучения в учебнике «Информатика и ИКТ».

В учебный материал входят темы:

История развития мобильного Интернета (телефонная связь; сотовая связь; первый мобильный телефон — создатель Мартин Купер; понятие мобильного устройства; классификация современных мобильных устройств);

Подключение к сетям и устройствам (подключение к мобильным сетям, сетям Wi-Fi, к устройствам Bluetooth, к компьютеру через USB, к виртуальным частным сетям (VPN), работа с сетификатами безопасности);

Защита информации на мобильном устройстве. Доступ к мобильному устройству (защита даннных об учётных записях; история СМС-переписки и телефонная книга; данные Web-браузера; защита содержимого карты памяти; защита от любопытных и кражи; атака вредоносного ПО; фишинговая атака).

Приложения

Для организации практической работы с мобильными устройствами пользуемся личными мобильными устройствами (телефонами, смартфонами, планшетами и т.д.) учащихся. В качестве примера применения современных достижений защиты мобильных устройств от угроз различного вида демонстрирую работу приложений, ViPNet Client iOS и ViPNet Client Android — это приложения, работающие под управлением операционной системы Apple iOS и Android, которые *обеспечивают:*
• защиту iPad, iPhone и мобильных устройств с ОС Android от сетевых атак;
• доступ посредством защищённого технологиями ViPNet VPN туннеля, к защищённым ресурсам сети;
• перехват любой IP трафик, обеспечивая его прозрачное шифрование [2].

Это ПО обеспечивает эффективную многоуровневую защиту мобильного устройства (антивирусная защита и контентная фильтрация), причём без установки дополнительного программного обеспечения на каждое мобильное устройство, что немаловажно, учитывая ограниченные возможности автономной работы мобильных устройств.

При демонстрации работы ViPNet на мобильном устройстве следует показать как используются различные конфигурации. *Конфигурация ViPNet Client для мобильных приложений* — это фиксированный набор параметров работы приложения, предназначенных для настройки параметров доступа к корпоративным ресурсам и ресурсам Интернета.

Мобильные приложения ViPNet используют конфигурации:
• *блокировать сеть* — блокировка всех соединений;
• *отключить защиту* — отключение обработки IP-трафика (соединение с защищёнными ресурсами невозможно, доступ к ресурсам Интернет разрешён, но при этом защита IP-трафика не осуществляется);
• *VPN и Интернет* — доступ к защищённым ресурсам и ресурсам Интернета (открытый трафик передаётся или через корпоративный прокси-сервер, или через координатор, защищённый трафик передаётся через координатор):
- Прямой доступ;
- Шлюзовой Координатор;
- Корпоративный прокси-сервер (предусмотрен только для мобильного приложения ViPNet Client for iOS).

Прямой доступ

При выборе этой конфигурации возможна работа с ресурсами защищённой сети ViPNet и прямой неограниченный доступ к открытым ресурсам Интернета. При работе в этой конфигурации нет возможности контролировать открытый трафик абонентского пункта, развёрнутого на устройстве.

Используйте конфигурацию для работы, например, в тех случаях, когда есть уверенность в том, что на устройстве отсутствует информация, к которой нежелателен доступ посторонних лиц.

Шлюзовой координатор

При выборе этой конфигурации работа с ресурсами защищённой сети ViPNet и доступ к открытым ресурсам Интернета осуществляются через *Координатор*, выполняющий роль сервера IP-адресов. При работе в конфигурации контролируется весь трафик абонентского пункта, развёрнутого на устройстве.

Использовать конфигурацию можно для работы, например, находясь в кафе или в аэропорту, предоставляющем мобильный доступ к ресурсам сети Интернет (Wi-Fi и 3G). Так как все соединения с узлами защищённой и открытой сетей осуществляются через координатор, для администратора точки доступа они будут невидимы, что исключает возможность перехвата трафика.

Корпоративный прокси-сервер

При выборе этой конфигурации все соединения с открытыми узлами осуществляются через защищённый прокси-сервер. Подключения к защищённым узлам ViPNet по протоколу HTTP требуется разрешить на прокси-сервере, подключение к защищённым узлам по другим протоколам не ограничено.

Соединение с прокси-сервером осуществляется по защищённому каналу, при этом на прокси-сервере осуществляется обработка трафика в соответствии с корпоративными политиками безопасности (например, защита от вирусов и сетевых атак).

Используют конфигурацию, например, при поездке в командировку, в которую необходимо взять с собой iPad для возможности обмена с коллегами различными служебными данными (например, презентациями, документами, электронными таблицами). При работе в конфигурации вся передаваемая информация будет защищена от несанкционированного доступа.

Набор конфигураций, доступный пользователю, зависит от уровня его полномочий, который задаёт администратор сети ViPNet.

Используя эти приложения, мы формируем у школьников системное представление: об угрозах, возникающих при использовании мобильных устройств; о способах и средствах защиты личной и другой информации, хранящейся на мобильных устройствах; о современных программно-аппаратных средствах защиты информации и возможном их применении для защиты мобильного устройства.

* * *

Практическое использование средств защиты информации в учебной деятельности повышает интерес школьников к этому направлению обучения, помогает при выборе профессии после получения среднего образования. **В$_{в}$Ш**

Источники

1. Symantec выявила новые виды мобильных угроз. [Электр.ресурс]. — URL: http://www.anti-malware.ru/news/. — Дата обращения: 06.05.2014 г.
2. ViPNet Client for Android. [Электр.ресурс]. — URL: http://infotecs.ru/. — Дата обращения: 01.05.2014г.
3. Интернет в России и мире. Пользователи Интернета в России. [Элект.ресурс.]. — URL: http://www.bizhit.ru/index/users_count/0–151. — Дата обращения: 02.05.2014г.
4. Мобильная экосистема. [Элект.ресурс.]. — URL: http://xiper.net. Мобильная экосистема. — Дата обращения: 02.10.2014 г.

5. Мобильное интернет-устройство. [Элект.ресурс.]. — URL: https://ru.wikipedia.org/wiki/ — Дата обращения: 02.05.2014 г.
6. Мобильные устройства [Элект.ресурс.]. — URL: http://letopisi.org/index.php/Мобильные_устройства — Дата обращения: 02.05.2014г.
7. Приостановка Воспроизведения Google. [Электр.ресурс]. — URL: https://www.bit9.com/. — Дата обращения: 06.05.2014 г.
8. Тысячи Android-приложений собирают персональные данные без разрешения [Электр. ресурс]. — URL: http://www.cnews.ru/. — Дата обращения: 06.05.2014 г.