Синица Александра Игоревна
учитель русского языка и литературы,
педагог дополнительного образования
ГБОУ СОШ №531 Красногвардейского района
г. Санкт-Петербург
Синица Александр Михайлович
педагог дополнительного образования
ГБОУ ДОД «Санкт-Петербургский центр
детского (юношеского) технического творчества»
г. Санкт-Петербург

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УСПЕШНОГО ПОЛЬЗОВАТЕЛЯ В СИСТЕМЕ ОБРАЗОВАНИЯ

Аннотация: *данная статья посвящена рассмотрению угроз глобальной сети и информационной безопасности. Материал может быть интересен преподавателям и учителям любого направления, так как безопасность работы с Интернетом важна для каждого, вне зависимости от возраста и положения.*

Ключевые слова: *электронные ресурсы, угрозы безопасности, интернет-ресурсы, способы борьбы.*

Современное образование не мыслит своего существования без обращения к электронным ресурсам. Однако насколько это небезопасно для пользователя не каждый понимает. Ведь про угрозы безопасности задумываемся мы порой поздно. В данной работе мы рассмотрим несколько видов угроз глобальной сети. При рассмотрении видов угроз сети «Интернет» необходимо разделить их источники:

1. Знакомые и доверенные интернет ресурсы (Социальные сети, e-mail, известные сайты с высоким уровнем доверия).

2. Незнакомые интернет ресурсы.

3. Сетевая инфраструктура (Wi-Fi роутеры, общедоступные точки доступа).

4. Другие источники, не связанные напрямую с сетью «Интернет» (флешки, переносные жесткие диски, установочные файлы программ).

5. 0day уязвимости (уязвимость нулевого дня) программного и аппаратного обеспечения. Новые и неизвестные разработчикам уязвимости (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё).

Перед выделением перечня угроз заметим, что любые незаконные и вредоносные действия выполняются разного рода программным обеспечением (в том числе с ручным управлением), являясь, таким образом, вредоносным программным обеспечением (вирусами), что является опасным для всей сети, если устройство заражено в учебном учреждении. Обозначим виды угроз:

1. Шифрование файлов и добавление баннеров (зачастую порнографического содержания) с целью вымогательства.

2. Добавление рекламных материалов (в том числе порнографического и эротического характера) в содержимое сторонних сайтов и/или интерфейс личных устройств.

3. Кража личных данных (в том числе учетных записей и данных банковских карт).

4. Установка стороннего дополнительного программного обеспечения (mail.ru спутник, Amigo, Yandex Браузер и пр.).

5. Использование вычислительных мощностей и/или полосы доступа в интернет компьютера (в том числе мобильных устройств) в личных целях злоумышленника.

6. Выведение из строя устройств пользователя, в том числе на физическом уровне.

Для эффективной борьбы с «врагом» его необходимо знать «в лицо». Практически все описанные ниже угрозы актуальны и для мобильных устройств, это необходимо оговорить, так как в школах появляется возможность работать с ЭФУ, то есть с электронными формами учебников, с оговоркой, что эффектив-

ного антивирусного программного обеспечения для мобильных устройств невозможно разработать в силу особенностей обеспечения безопасности мобильных операционных систем. Таким образом единственный способ защиты от любого вида заражения – это запрет установки приложений из любых источников кроме доверенного. Рассмотрим некоторые виды угроз подробнее.

Чуть менее опасный и более старый, но работающий и имеющий вид вредоносного программного обеспечения – размещение баннеров (WinLock). Принцип работы заключается в добавлении поверх интерфейса провокационных (часто порнографических или угрожающих) баннеров с требованием отправить СМС для получения кода разблокировки. Из-за того, что данный вид вирусов достаточно старый, антивирусное программное обеспечение способно достаточно эффективно бороться с заражением подобного рода. Если же заражение по какой-то причине все же произошло, то существует сервис разблокировки компьютеров, также, возможно, поможет использование лечащей утилиты или загрузочного диска восстановления операционной системы, а также отката операционной системы к точке восстановления. Отправка СМС зачастую бесполезна, так как поддержка этих вирусов, скорее всего, давно прекращена. Заражение производится, в основном, с помощью вложений в e-mail или загружаемого содержимого (презентации, пиратское ПО, музыка и прочее).

Отметим следующую угрозу – установка стороннего дополнительного программного обеспечения. Такая активность является не сколько вирусной, сколько рекламной: установка обычно производится, формально, с разрешения самого пользователя. В результате может привести к значительному замедлению скорости работы персонального компьютера. Ситуацию осложняет также то, что установка дополнительного программного обеспечения, обычно, не требует прав администратора. Наиболее эффективным способом борьбы является минимизация установок различного бесплатного программного обеспечения, установка программного обеспечения в режиме Advanced (для продвинутых пользователей) с внимательным прочтение всех шагов установки и отказом от установки

дополнительного программного обеспечения, а также полного отказа от установки и загрузки любого контента из недоверенных источников.

Один из самых древних видов компьютерных вирусов, появившихся ради развлечения – это выведение из строя устройств пользователя, в том числе на физическом уровне. На данный момент не имеет широкого распространения и эффективно подавляются антивирусами и средствами операционных систем. Заражение таким вирусом потенциально приводит к потере файлов или повреждению устройств, обычно без возможности восстановления. Такие вирусы часто встречаются на компьютерах с широким доступом (университеты, интернет-кафе).

При использовании интернет-ресурсов необходимо помнить, что опасность может прийти с любой стороны, в том числе от ваших друзей и коллег. Относитесь с подозрением к любым сообщениям (в том числе e-mail), содержащим вложения файлов и ссылок, по возможности подтвердите отправку файлов по достоверным каналам связи (телефон, другой интерне-сервис). Помните, что заражение возможно не только через исполняемый файл-программу, но и через любой документ и даже картинку.

В качестве сервиса электронной почты желательно использовать те, где минимум нет рекламных баннеров в интерфейсе почты, заражение может произойти и через баннер. Внимательно следите за интернет адресом страницы, где вводите данные для авторизации, часто используются похожие адреса (например mai1,ru вместо mail.ru 1(один) вместо l (L).Обязательно включайте двухфакторную аутентификацию, которая позволит обезопасить вашу учетную запись, даже при утечке пароля.

Следите за состоянием защищенного подключения, используйте всегда https, следите, чтобы браузер считал соединение достоверным. Никогда не устанавливайте никаких удостоверяющих сертификатов.

Важно помнить, что предупрежден – значит, защищен. Необходимо объяснять своим подопечным об уязвимости в глобальной сети и о том, как защитить себя от подобных угроз.

Список литературы

1. Памятка по безопасному использованию глобальной сети Интернет для чайников [Электронный ресурс]. – Режим доступа: http://san-tit.blogspot.ru/2016/02/blog-post.html