УГРОЗЫ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ ДЛЯ ПОДРОСТКОВ

Лежнев А.А.

г.о. Люберцы, МОУ «СОШ №27», 11 «А» класс

Руководитель: Лежнева О.Б., г.о. Люберцы, МОУ «СОШ №27», учитель информатики и ИКТ первой квалификационной категории

Цель проекта – сформировать у подростков активную позицию в получении знаний и умений выявлять угрозу в сети Интернет, определять степень ее опасности, предвидеть последствия угрозы и противостоять ей.

Задачи проекта:

– формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности,

– формирование навыков оценки опасных ситуаций при использовании сети Интернет.

Актуальность:

– безопасность в глобальной сети Интернет является одной из главных проблем, с которой сталкивается современное общество, в том числе и подростки. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации. При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть при определенных условиях открыты всем, кто обладает необходимыми средствами.

Для сбора данных мы использовали опрос**,** проведенный с помощью Google Форм среди учеников средней и старшей школы МОУ СОШ 27, а также подростков, проживающих на территории РФ и за её пределами.

Мошенники и киберпреступники

В наше время среди подростков очень популярны соц. сети. Через страницы в любой соц. сети можно узнать личную информацию о ее пользователе и этим пользуются всякого рода мошенники. Для таких целей они используют «фишинг».

«Фишинг» представляет собой сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Это может осуществляться при помощи спама, почтовых и мгновенных сообщений, вредоносных интернет-сайтов. Главная задача «фишинга» – получение логина и пароля пользователя для определённого сайта, с дальнейшим их использованием.

Также современные подростки используют интернет как рабочую и торговую площадку. Они создают какого-либо рода услуги и обмениваются ими с пользователями за определенную плату на привязанные к учетной записи кредитным картам и электронным кошелькам. Для воровства данных о кредитных картах и кошельках также используется «фишинг»

Главным типом кибермошенничества является создание и ведение сайтов-казино и бинарных опционов. Такие сайты при помощи определенных запрограммированных алгоритмов или искусственного интеллекта во время игры на автомате или виртуальном поединке игроков выманивают валюту, приобретенную за деньги, с привязанных к сайту аккаунтов.

Из анализа опроса по данному виду угроз следует, что 40% респондентов когда-либо становились жертвами мошенников и киберпреступников (Приложение 1).

Анонимайзеры и брандмауэры

Любому компьютерному терминалу или мобильному устройству при входе в интернет присваивается уникальный идентификатор в виде внешнего IP-адреса. И в мире такие адреса не повторяются. Иными словами, каждое устройство имеет заранее строго определенный код, по которому можно вычислить его местоположение. Для того, чтобы остаться неузнанным в Сети, необходимо скрыть IP-адрес или подменить его на какой-то другой, неиспользуемый в данный момент. Эти процессы обеспечивает анонимайзер. В целом его функционирование несколько напоминает то, как работают анонимные прокси-серверы, которые по большому счету тоже можно отнести к одному из подвидов данного типа программ и сервисов. При использовании данной технологии IP-адрес вашего компьютера, присвоенный провайдером, меняется сервисом анонимайзера на свободный IP-адрес по усмотрению пользователя. Таким образом, пользователь может защитить свой аккаунт от хакеров и корпораций, занимающихся незаконной деятельностью, и спецслужб.

В результате опроса мы выяснили, что 50% респондентов не только знают, что та-

кое анонимайзеры, но и предпочитают работать в купе с ними (Приложение 2).

TORRENT и нелицензионный контент

BitTorrent (или торрент-трекер) – это протокол, разработанный для обмена файлами через Интернет. Особенностью данного протокола является применение принципа P2P (peer-to-peer). Благодаря использованию этого принципа, данные могут передаваться не только от источника к получателю, но и от одного получателя к другому. Таким образом, значительно снижается нагрузка на источник данных и данные можно передать всем желающим значительно быстрее.

На практике передача происходит так. Распространение файла с помощью BitTorrent идет по частям. После того как получатель скачал часть файла, он может начать скачивать следующую часть файла, при этом одновременно передавать уже полученные части файла другим желающим. Аналогичным образом работают все остальные участники сети. Это позволяет передать один и тот же файл большому количеству пользователей с очень большой скоростью.

По сути Торрент-сайты не несут ответственности за загруженный торрент-файл, принадлежащего другому пользователю, и поэтому в таком файле может содержаться спам, вирус, либо этот файл является «фишинг»-ссылкой.

Наш опрос на гугл-формах показал, что 37% респондентов пользуются торрент-трекерами (Приложение 3).

Компьютерные вирусы

Компьютерный вирус – это программное обеспечение с возможностями самокопирования, внедрения в системный код и другие программные продукты, а также нанесения непоправимого ущерба аппаратной части компьютера и информации, хранящейся на его носителях. Вредоносное программное обеспечение получило название «вирус» за свое сходство с биологическим прототипом. Он так же может иметь стадию инкубации, и так же самостоятельно размножается и паразитирует в операционной системе компьютера.

Таким образом, компьютерным вирусом является ПО с опасными для систем машины свойствами. Основная цель любого вируса – нанесение вреда, хищение информации или наблюдение за компьютером. Также прослеживаются и другие действия компьютерных вирусов. Склонность к размножению позволяет нанести максимальный урон.

В результате проведенного опроса мы выяснили, что 32% респондентов часто сталкиваются с компьютерными вирусами (Приложение 4).

Криптовалюта

Криптовалютой называют особую разновидность электронного платежного средства. Строго говоря, это математический код. Называется она так из-за того, что при обращении этих цифровых денег используются криптографические элементы, а именно электронная подпись.

Единицей измерения в этой системе считаются «коины» (буквально – «монеты»). Криптовалюта не имеет никакого реального выражения типа металлических монет или бумажных банкнот. Эти деньги существуют исключительно в цифровом виде.

«Выпуск» цифровых денег происходит различными способами: это и ICO (первичное размещение монет, система инвестирования), майнинг (поддержание специальной платформы для создания валюты), и форжинг (образование новых блоков в уже имеющихся криптовалютах). То есть криптовалюта возникает буквально «из интернета».

Так как есть много видов криптовалюты, создание которой не требует больших усилий или дорогого технического оснащения, подростки стали заниматься ее созданием и пампингом. Главная ее проблема в том, что криптовалюта хранится на определенном сервере и отследить пропажу или воровство этих денег могут только службы защиты. Хакеры, которые украли коины с принадлежащим другому человеку математическим кодом используют эти деньги для противозаконных целей от лица другого человека.

По результатам опроса 39% респондентов даже не знакомы с понятием криптовалюта, в то время как 53% знают, что это такое, а 8% работают с ней (Приложение 5).

Заключение

Способы защиты от угроз в глобальной сети Интернет:

- загрузить антивирусные программы (для обеспечения наибольшей безопасности лучше загрузить платную антивирусную программу) и firewall и регулярно их обновлять
- шифровать свои электронные кошельки, кредитные карты и блоки криптовалюты
- пользоваться анонимайзерами во время работы в Интернете
- пользоваться только проверенными сайтами
- ставить пароли с различным набором символов клавиатуры на свое устройство и учетные записи, исключая персональную информацию (даты рождения и т.п.)
- не открывать подозрительные ссылки или случайно установленные на устройство

программы, включая файлы с разрешением «.exe»

• использовать межсетевой экран для регулярного отслеживания своих сеансов в глобальной сети Интернет

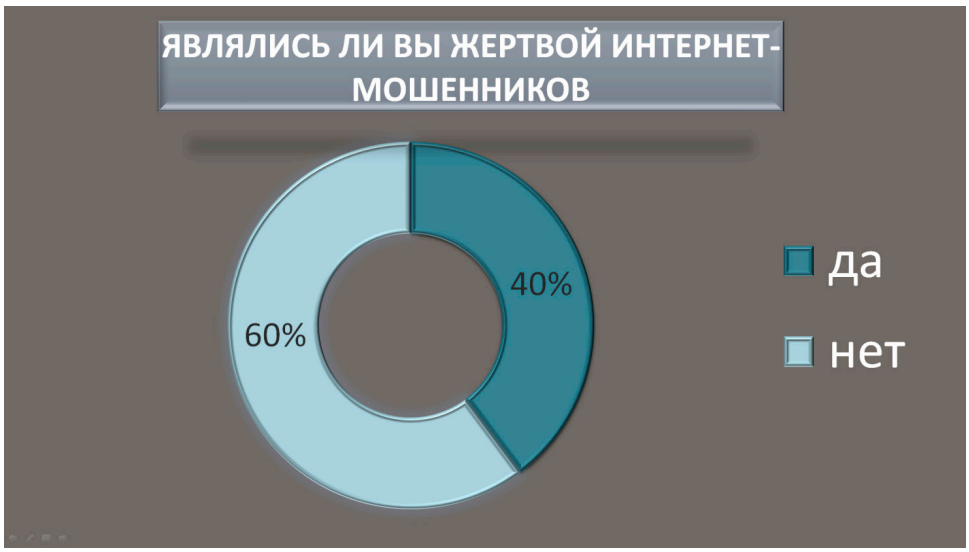
• обращать внимание на адресную ссылку сайтов (URL в адресной строке должен совпадать с названием WEB-страницы, на которой вы находитесь).

Список литературы

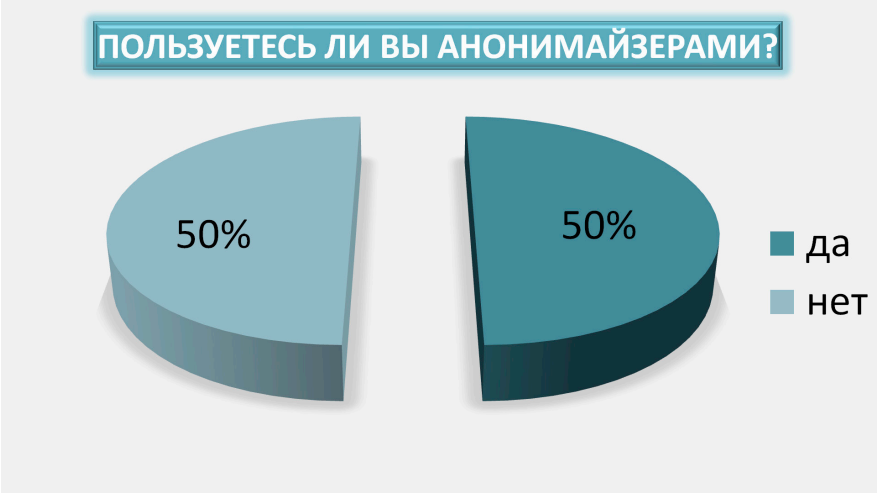
1. https://docs.google.com/forms/d/e/1FAIpQLScwyNfaWGPA1hmu0F3C4MhV5YqaTR0g8FRfFhyayYwAlPDFWQ/viewform?usp=sf_link (Опрос на Google-Формах).
2. http://comp-security.net.
3. http://kakzarabativat.ru/finansy/chto-takoe-kriptovalyuta/.
4. http://comp-security.net/.
5. https://www.syl.ru/article/174954/new_chto-takoe-kompyuternyiy-virus-vidyi-kompyuternyih-virusov-zaschita-ot-kompyuternyih-virusov.

Приложения

Приложение 1



Приложение 2



Приложение 3

Приложение 4

Приложение 5