УДК 004.738.5

КИБЕРУГРОЗЫ И КИБЕРБЕЗОПАСНОСТЬ ОБЫЧНОГО ПОЛЬЗОВАТЕЛЯ ИНТЕРНЕТ

Татьяна Петровна Почтарькова
преподаватель
pltp@mail.ru
Вадим Вадимович Пащенко
студент
vadim21436587vadim@gmail.com
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматривается вопрос безопасного использования сети Интернет обычным пользователем. Выделены наиболее распространенные киберугрозы, источники киберпреступлений и даны рекомендации по защите от них.

Ключевые слова: интернет, частные пользователи, угрозы, источники киберпреступлений, способы защиты.

Интернет стал неотъемлемой частью жизни современного человека. Глобальная Сеть охватила своей паутиной все континенты и страны, проникла во все сферы жизни. Через Интернет решаются вопросы, начиная от вызова такси и заказа пиццы, заканчивая многомиллионными сделками. В настоящее время в электронном виде есть практически вся информация о каждом из нас — паспортные данные, десятки или сотни фотографий, денежные средства на карточках или электронных кошельках. И этот факт является очень привлекательным для мошенников. Получая обманным путем конфиденциальные данные простых граждан, хакеры создают им большие проблемы: от потери репутации до получения чужих кредитов или опустошения банковских счетов. Понимание того, какие киберугрозы существуют и как от них защитится, поможет рядовому пользователю находится в сети Интернет более уверенно.

Целью нашей работы стало изучение киберугроз, которые могут подстерегать современного пользователя сети Интернет, и способов защиты от них. В соответствии с поставленной целью предстояло решить следующие задачи: 1) Изучить литературу и интернет-источники по данной теме; 2) Изучить статистику кибератак на частных пользователей за последние несколько лет; 3) Разработать рекомендации по безопасной работе в сети Интернет.

Кибератака, или киберугроза, — это любое злонамеренное действие, направленное на повреждение, кражу или тайное изменение данных. Кибербезопасность — это защита подключенных к интернету систем (оборудования, программного обеспечения и данных) от киберугроз.

Основные типы угроз, с которыми борется современная кибербезопасность, и которые могут коснуться частных пользователей сети:

1. *Вредоносное программное обеспечение (ВПО*) - самый распространенный инструмент киберпреступников. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Вредоносные программы крадут, шифруют и удаляют конфиденциальные

данные, изменяют или захватывают основные вычислительные функции и отслеживают активность компьютеров или приложений. Вредоносное ПО может быть самым разным, вот некоторые распространенные виды: *Вирусы* – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя. *Троянцы* – вредоносы, которые прячутся под маской легального ПО. Они собирают данные или повреждают их. *Шпионское ПО* – программы, которые втайне следят за действиями пользователя и собирают информацию. *Программы-вымогатели* шифруют либо всю операционную систему, либо отдельные файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.

2. *Социальная инженерия.* Метод атак, основанный на человеческом взаимодействии. Злоумышленники втираются в доверие к пользователям и вынуждают их нарушить процедуры безопасности, выдать конфиденциальную информацию, например, мошеннические звонки по телефону с целью получить банковские данные.

3. *Фишинг.* Форма социальной инженерии. Мошенники рассылают пользователям электронные письма или текстовые сообщения, напоминающие сообщения из доверенных источников. При массовых фишинговых атаках злоумышленники выманивают у пользователей данные банковских карт или учетные данные. *Спам* является частью фишинга.

4. *Прямой взлом аккаунта.* Злоумышленник подбирает пароль, заходит к вам на страничку и творит всё, что заблагорассудится.

5. *Сталкерское ПО.* Предназначено для скрытой слежки за пользователями. Сталкерские приложения часто распространяются под видом легального ПО. Такие программы позволяют злоумышленникам просматривать фотографии и файлы на устройстве жертвы, подглядывать через камеру смартфона в режиме реального времени, узнавать информацию о местоположении, читать переписку в мессенджерах и записывать разговоры.

6. *Криптоджекинг.* Относительно новый тип киберпреступлений, при которых вредоносное ПО скрывается в системе и похищает вычислительные ресурсы устройства, чтобы злоумышленники могли их использовать для добычи криптовалюты. Процесс криптоджекинга полностью скрыт от глаз пользователей. Большинство жертв начинают подозревать неладное, только заметив увеличение счетов за электроэнергию.

7. *Онлайн-груминг.* Грумингом называют различные виды мошенничества в сети, когда преступники обманом втираются в доверие к пользователям и получают от них личные данные или деньги за несуществующие товары и услуги.

8. *Атаки Man-in-the-Middle* («человек посередине»). Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, подключившись к незащищенной сети Wi-Fi.

9. *Ботнеты.* Киберпреступники используют специальные троянские программы, чтобы обойти систему защиты компьютеров, получить контроль над ними и объединить их в единую сеть (ботнет), которой можно управлять удаленно. «Зомби-сети» используют для накрутки рекламных постов, распространения пропаганды и фейков, крупномасштабных кампаний по рассылке спама и других типов кибератак.

10. *Межсайтовый скриптинг.* Преступники добавляют вредоносный скрипт, например, JavaScript-сниффер, в обычный сайт. А затем программное обеспечение может записывать вашу конфиденциальную информацию, данные, которые вы вводите при входе на этот сайт.

11. *Кибербуллинг.* Травля по интернету — это угрозы и оскорбления от агрессивно настроенных пользователей в адрес другого пользователя в различной форме и по любой причине.

В качестве основных источников киберпреступлений в сфере защиты персональных данных Роскомнадзор выделяет следующие: принятие субъектом

пользовательских соглашений по умолчанию; использование "серых" мобильных приложений; передача персональных данных по незащищенным каналам связи; использование геолокационных сервисов; распространение своих персональных данных в открытых источниках; общение с незнакомыми людьми в соцсетях и др.

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Число вредоносных объектов, которые обнаруживаются в сети ежегодно, исчисляется миллиардами. Каждый год это число увеличивается на 40%. Атаки в информационном пространстве наносят ущерб, который оценивается в сотни миллиардов долларов. По заявлению начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова каждую секунду 12 человек на Земле становятся жертвами киберпреступников. Согласно данным Росстата, 22% пользователей сталкивались с кражей аккаунтов в социальных сетях или играх; 15% теряли данные из-за компьютерного вируса; 14% отметили, что им писали странные сообщения; 10% сталкивались с мошенничеством с использованием фальшивых сайтов и писем. В 2020 году россияне лишились около 9 млрд рублей из-за действий кибермошенников. По данным ЦБ, две трети граждан, попавшихся на их уловки, относятся к экономически активному населению, и только одну треть жертв составили пенсионеры. 2022 год запомнился масштабными утечками данных. Количество атак на частных лиц увеличилось на 44%. На обычных пользователей пришлось 17% от числа всех атак. При этом преступники использовали различные приемы социальной инженерии в 93% случаев; создавали фишинговые сайты (56%), отправляли вредоносные письма по электронной почте (39%), искали жертв в социальных сетях (21%) и мессенджерах (18%). В 64% атак злоумышленникам удавалось украсть данные. В основном это были учетные данные (41% среди украденной информации), персональные (28%) и платежные (15%). Пользователи также стали жертвами множества утечек данных, которые произошли в крупных компаниях и популярных сервисах, в числе которых Яндекс.Еда, «ВкусВилл», Whoosh,

«СДЭК», Delivery Club, «Гемотест», DNS. По данным Роскомнадзора, произошло не менее 60 крупных утечек персональных данных, содержащих более 230 млн записей с личной информацией граждан.

Количество атак на частных лиц продолжает расти. Преступники продолжают использовать неграмотность людей в вопросах обеспечения собственной информационной безопасности. Как выяснилось, планомерной государственной программы по повышению осведомленности граждан в вопросах кибербезопасности пока не существует. Чтобы защитить личную информацию в интернете и минимизировать риски, мы рекомендуем следующие действия:

1) Обновите программное обеспечение и операционную систему. Используйте антивирусные программы. Своевременно обновляйте браузер.

2) Храните минимум личной информации в сети.

3) Используйте двухфакторную аутентификацию.

4) Избавляйтесь от метаданных. Отключите в вашем смартфоне выставление геометки при фото и видеосъемке.

5) Отказывайтесь от сбора «куки» и используйте режим инкогнито. При установке приложений или регистрации на сайте не выдавайте разрешений распоряжаться вашими личными данными. Не открывайте доступ к камере, фотогалерее и микрофону.

6) Генерируйте сложные пароли. Не используйте одинаковые пароли на разных сайтах. Регулярно меняйте пароли. Не храните пароли в браузере и даже специальном менеджере. Не разрешайте браузеру автоматически запоминать пароли к личным сайтам и страницам. Отключите синхронизацию браузера на компьютере и в смартфоне.

7) Высылая сканы документов через электронную почту, удаляйте их сразу же или установите дополнительно пароль на папку «Исходящие».

8) Не открывайте почтовые вложения от неизвестных отправителей. Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов.

9) Заведите себе несколько адресов электронной почты: для личной корреспонденции и публичный адрес. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

10) Избегайте незащищенных сетей Wi-Fi в общественных местах, не заходите через них на сайты, которые требуют ввода паролей и личных данных. В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Отключайте Bluetooth, когда им не пользуетесь.

11) Удаляйте файлы cookies на компьютере и в смартфоне. Благодаря cookies сайты помнят ваши логины, пароли, электронную почту.

12) Используйте сайты, имеющие защищённое соединение, в которых информация недоступна для третьих лиц. У таких сайтов в адресной строке браузера перед адресом сайта https:// зелёный замочек.

13) Установите блокировщик рекламы. Специальные программы, блокирующие рекламу, одновременно отслеживают попытки посторонних программ получить информацию с вашего компьютера.

14) Чтобы не пострадать от кибербулинга, соблюдайте несколько правил: не отвечайте на агрессивные сообщения; занесите обидчиков в чёрный список; сообщите о происходящем технической поддержке социальной сети; делайте скриншоты переписки, содержащей оскорбления и угрозы.

Представленные рекомендации не гарантируют абсолютную анонимность или полную защиту личных данных. Остаться полностью анонимным в сети проблематично. Однако, чем больше о вас знает интернет, тем выше риск.

Список литературы:

1. Северин В. А. Актуальные вопросы правового регулирования и защиты информации в России: избранные труды // Москва: URSS: Ленанд. 2022. 474 с

2. Проблемы правовой и технической защиты информации: сборник статей / Алтайский государственный университет; редакционная коллегия: Поляков В.В., проф., д.ф.-м.н. - главный редактор [и др.] / Барнаул: Изд-во Алтайского государственного университета. 2021. 69 с.

UDC 004.738.5

CYBER THREATS AND CYBERSECURITY OF AN ORDINARY INTERNET USER

Tatiana P. Pochtarkova
teacher
pltp@mail.ru
Vadim V. Pashchenko
student
vadim21436587vadim@gmail.com
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. The article discusses the issue of safe use of the Internet by an ordinary user. The most common cyber threats, sources of cybercrime are identified and recommendations for protection against them are given.

Key words: internet, private users, threats, sources of cybercrime, methods of protection.

Статья поступила в редакцию 30.03.2023; одобрена после рецензирования 30.05.2022; принята к публикации 30.06.2023.

The article was submitted 30.03.2023; approved after reviewing 30.05.2022; accepted for publication 30.06.2023.