УДК 004.056

КАК ОБЕЗОПАСИТЬ СЕБЯ В СЕТИ ИНТЕРНЕТ

О. В. Акимин, К. И. Юрченко, С. К. Гавриленко
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. В 2021 году в России было зарегистрировано около 518 тысяч киберпреступлений, а год спустя это количество снизилось на 1,8 %. Данный факт может свидетельствовать о том, что люди становятся более киберграмотными, учатся сохранять свои личные данные при пользовании Интернетом. Но тем не менее проблема безопасности еще далеко не решена, по-прежнему существует опасность заразить свой компьютер вредоносными вирусами, утерять личные данные. Авторы данной статьи пытаются на своем уровне решить часть этой глобальной проблемы, их цель — дать рекомендации пользователям Всемирной паутины, как обезопасить себя, входя в Интернет, как зашифровать свой компьютер, организовать менеджмент паролей, они уточняют, какие антивирусы лучше использовать, рассказывают о преимуществах протокола HTTPS и о том, как избегать фишинговые сайты.

Ключевые слова: безопасность, шифрование, https, антивирусы, защита, пароли, двухфакторная авторизация, конфиденциальность, анонимные сети.

HOW TO PROTECT YOURSELF ON THE INTERNET

Oleg V. Akimin, Kirill I. Yurchenko, Sergey K. Gavrilenko
Don State Technical University (Rostov-on-Don, Russian Federation)

Abstract. In 2021, about 518 thousand cybercrimes were registered in Russia, and a year later this number decreased by 1.8%. This fact may indicate that people are becoming more cyber-literate, learning to protect their personal data when using the Internet. But nevertheless, the security problem is far from being solved. There is still a danger of infecting your computer with malicious viruses, losing personal data. The authors of this article are trying to solve part of this global problem at their level. Their goal is to give recommendations to users of the World Wide Web, how to protect themselves by logging into the Internet, how to encrypt the computer, organize password management. They specify which antiviruses are better to use, talk about the advantages of the HTTPS protocol and how to avoid phishing sites.

Keywords: security, encryption, https, antiviruses, protection, passwords, two-factor authentication, confidentiality, anonymous networks.

Введение. Личная информация пользователей Интернета (будь то просто номер телефона, паспортные данные или даже номера банковских карт) может по той или иной причине попасть в открытый доступ, это нанесет вред человеку, если ею воспользуются злоумышленники. Чтобы такого не случилось, надо уметь противостоять подобным рискам, а для этого нужно следовать нескольким важным советам. В данной статье речь, в частности, пойдет о способах защиты личных данных от посторонних лиц. Будут рассмотрены шифратор логических дисков DiskCryptor, менеджер паролей KeePassX, антивирусные программы.

Основная часть. Большинство пользователей хранит свои данные, конфиденциальную информацию на персональных компьютерах и смартфонах, не думая о том, что их не так сложно украсть или скопировать с них информацию. Чтобы такого не произошло, следует использовать шифрование.

Самый правильный способ — это зашифровать не только какую-то определенную информацию, но всю. Многие устройства поддерживают полное шифрование.

Установка DiskCryptor.

1. Для загрузки программы DiskCryptor зайдите на страницу по адресу: github.com/DavidXanatos/DiskCryptor/releases, щелкните мышью на ссылке dcrypt_setup_1.2_beta_3_signed.exe и сохраните файл на компьютер.

2. Запустите установщик и установите программу. Иногда приходится запускать его с правами админа, кликните по файлу правой кнопкой мыши и кликните на пункт «Запустить от имени администратора» из контекстного меню.

3. Перезагрузите компьютер, чтобы завершить процесс установки, это необходимо для начала работы программы.

После шифрования данных устройства вы сильно усложните работу злоумышленнику, который захотел получить вашу информацию, он даже не узнает, что хранится на вашем компьютере. Чтобы зашифровать данные жесткого диска, следует выполнить следующие шаги:

1. Запустите DiskCryptor.

2. В списке «Диски» выберите необходимый вам диск (например D:) и кликните на кнопку «Шифровать» в правом верхнем углу программы.

3. Оставьте параметры по умолчанию и кликните «Далее» и ещё раз «Далее».

4. Выбрав безопасный пароль, введите его в поле «Пароль» и кликните «Подтверждение», а затем «ОК».

5. Шифрование занимает немного времени, по его завершению перезагрузите устройство.

После выполнения этих пунктов данные на вашем диске будут зашифрованы. Для обратного действия снова запустите DiskCryptor, выберите зашифрованный вами диск и нажмите на кнопку «Расшифровать». Имейте в виду, что ваши данные защищены только тогда, когда компьютер выключен, в ином случае злоумышленник сможет получить доступ к вашей информации [1].

Пользователи проводят много времени в Интернете, как правило, зарегистрированы на многих сайтах и имеют несколько аккаунтов. Если вы используете для них одинаковые или похожие пароли, то злоумышленнику не составит труда при взломе получить доступ сразу ко всем учетным записям. Такие случаи происходят весьма часто, поэтому, чтобы обезопасить себя, нужно использовать разные и сложные пароли для различных сайтов. Не стоит придумывать пароли вроде 1234 или qwerty, их легко подобрать. Хороший логин и пароль — это сложная комбинация, в которой используются заглавные и строчные буквы, цифры и символы. Для этой цели лучше задействовать специальные программы, которые генерируют их, например https://1password.com/ru/password-generator/

Очевидно, что сложные пароли трудно запомнить, поэтому следует воспользоваться следующими способами.

Первый способ — использовать специальную книжку для записи паролей, это чрезвычайно удобно и практично записывать и хранить пароли в надежном месте. Если ваши записи украдут, вы легко это заметите и быстро смените все пароли.

Второй способ — использование менеджера паролей. Это программа, которая дает возможность создавать, хранить, предоставлять сложные пароли при авторизации на сайтах и в приложениях.

Примером такой программы является KeePassX. Она позволяет хранить все пароли в одном месте. Необходимо помнить лишь один пароль (мастер-пароль), который нужен для доступа к

остальным. Скачать дистрибутив программы KeePassX можно с сайта keepassx.org/downloads.

Антивирусы — это, пожалуй, самый действенный способ борьбы с вирусами. На каждом компьютере и мобильном устройстве рекомендуется установить и постоянно обновлять антивирусную программу. Многие антивирусные комплексы представляют собой очень эффективные системы по защите устройств от вредоносных программ. Они не только удалят уже существующий вирус, но и предотвратят появление новых. Также помогут не переходить на опасные сайты, которые могут украсть ваши данные. Конечно, большинство антивирусов платные, однако есть и бесплатные достойные антивирусы. Например антивирус Касперского, он платный, однако есть и его бесплатная версия, ее можно скачать по ссылке www.kaspersky.ru/free-antivirus [1, 2].

О ссылках. Не нужно переходить по подозрительным ссылкам, даже если их отправил знакомый или близкий друг, нужно всегда обращать внимание на то, что написано в адресной строке сайта. Если адрес сайта начинается с HTTPS (например https://vk.com/feed), то все в порядке, это безопасное соединение, на данном сайте можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP (например http://government.ru), это значит, что соединение не защищено и вводить свои данные на этом сайте не рекомендуется. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию о сайте во всплывающем окне.

Не следует использовать общедоступные сети. Их часто можно встретить в торговых центрах, ресторанах или кафе. Не надо использовать их, если вы собираетесь вводить свои конфиденциальные данные или совершать покупку в онлайн-магазинах. В таких сетях злоумышленники могут украсть ваши данные.

В сети Интернет распространены такие виды мошенничества, как сайты-подделки, распространяющие вирусы и навязывающие платные услуги, мошенничество с использованием банковских карт, фишинговые сообщения, отправленные от имени администраторов банковских или других платежных систем, призывающие пользователей пройти по фальшивой ссылке на сайт, ставящий под угрозу конфиденциальные данные пользователя [3].

Фишинговый сайт — это сайт, который частично или полностью подделан. Мишенью таких сайтов являются ваши логины и пароли, которые вы вводите на оригинальных сайтах, фишинговый сайт легко отличить по доменному имени, например vk.com — официальный сайт, а vk.som — нет. Также есть сомнительные приложения, и неопытные пользователи могут скачать поддельное приложение банка, ввести туда свои данные и потерять деньги, поэтому всегда скачивайте приложения из надежных источников. Такими являются официальные магазины Google, Microsoft, Apple и других подобных компаний.

При посещении сайтов можно использовать прокси-сервер или анонимайзер, они используются с целью сохранения анонимности в сети Интернет, если нужно разово скрыть свой IP-адрес, зайти на заблокированный сайт или зашифровать передаваемую информацию [4].

Заключение. Рассмотренные в статье способы защиты личной, конфиденциальной информации в сети Интернет от посторонних лиц, злоумышленников не вызывают особых трудностей у пользователей Всемирной паутины. Не стоит только пренебрегать ими, игнорировать требования безопасности. Из-за собственной беззаботности, незнания основ кибербезопасности пользователь может понести невосполнимые потери.

Библиографический список

1. Райтман, М. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета / М. Райтман. — Санкт-Петербург : БХВ-Петербург, 2017. — С. 62–70.

2. Информационная безопасность / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев. — Нижний Новгород : ННГУ, 2017. — С. 126–127.

3. Интернет-безопасность без проблем. Совместный план для педагогов, родителей и детей / Л. В. Шарова, А. В. Анисимов, Н. А. Федотова, Е. Л. Шелковой. — Москва : Изд. АВТОР, 2020. — С. 17.

4. Колисниченко, Д. Н. Анонимность и безопасность в Интернете. От «чайника» к пользователю / Д. Н. Колисниченко. — Санкт-Петербург : БХВ-Петербург, 2012. — С. 6–7.

Об авторах:

Акимин Олег Викторович, студент кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), akimin97@mail.ru

Юрченко Кирилл Иванович, студент кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), kirill.yurchenko.2017@mail.ru

Гавриленко Сергей Константинович, студент кафедры «Вычислительные системы и информационная безопасность» факультета «Информатика и вычислительная техника» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), Postov.serjio@gmail.com

About the Authors:

Akimin, Oleg V., student of the Computer Engineering and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), akimin97@mail.ru

Yurchenko, Kirill I., student of the Computer Engineering and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), kirill.yurchenko.2017@mail.ru

Gavrilenko, Sergey K., student of the Computer Engineering and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), Postov.serjio@gmail.com