ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Чернобаев С.В.
Российский экономический университет имени Г.В. Плеханова (117997, г. Москва, Стремянный переулок дом 36). e-mail: chernobaev_serzh@mail.ru

В статье рассматривается необходимость защиты персональных данных в социальных сетях. Выкладывая различные фотографии, оставляя различные публикации на своих страницах социальных сетей, а также ведя переписку с друзьями, коллегами или знакомыми, мы автоматически оставляем о себе информацию, которая может быть использована против нас. Эта информация может являться нашими персональными данными, а для них необходима защита от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования. Многие не воспринимают это всерьёз, и потом жалеют об этом. Ведь, если информация личного характера окажется в руках злоумышленников, то это может привести к печальным последствиям; может быть нанесен огромный ущерб, в том числе и удар по репутации. В статье приведены необходимые рекомендации, которые помогут пользователям социальных сетей улучшить защиту персональных данных.

Ключевые слова: защита, персональные, данные, преступление, социальные, сети, угроза, копирование, блокирование, пароль, информация.

PERSONAL DATA PROTECTION IN SOCIAL NETWORKS

CHERNOBAEV S.V.

1 st year student Plekhanov Russian University of Economics. Stremyanny lane 36, Moscow, 117997, Russia. e-mail: chernobaev_serzh@mail.ru

The article discusses the need to protect personal data in social networks. Laying out the different photos, leaving various publications on their social media pages and leading correspondence with friends, colleagues or acquaintances, we will automatically leave information about themselves, which can be used against us. This information could be of our personal data, and they require protection from unauthorized or accidental access, destruction, alteration, blocking, copying. Many people do not take it seriously, and then regret it. After all, if personal information will be in the hands of criminals, could lead to tragic consequences; it can be a large loss, including a blow to the reputation. The article provides the necessary guidelines to help users of social networks to improve the protection of personal data.

Keywords: defense, personal, data, crime, social, network, threat, copying, blocking, password, information.

Уже не для кого ни секрет, что на сегодняшний день человек слишком много времени проводит за компьютером. аще всего он проводит это время в Интернете. Некоторые люди так работают, но большинство просто тратит своё время на общение в социальных сетях, таких как: «*ВКонтакте*», «*Одноклассники*», «*Facebook*», «Instagram», «*Twitter*» и т.д. Например, израильтяне проводят в социальных сетях 10,7 часа в месяц. На втором месте россияне – мы проводим в социальных сетях 10,3 часа в месяц. Проводя такое огромное количество времени в социальных сетях, невозможно не оставить о себе хоть какую-то личную информацию. Выкладывая различные фотографии, оставляя различные публикации на своих страницах, ведя переписку, мы автоматически оставляем о себе информацию, которая может быть использована против нас. В данном случае эта информация является *персональными данными*, для которых необходима защита. Многие не воспринимают это всерьёз, и потом жалеют об этом. Ведь, если информация личного характера окажется в

руках злоумышленников, то это может привести к печальным последствиям. Например, самое распространённое - это **шантаж**. Получив конфиденциальную информацию о вас, злоумышленники тут же пытаются извлечь из этого выгоду (деньги, различные ценности и т.д.). Конечно же, никто не хочет, чтобы его личную информацию разглашали всем, будь то переписка, или фотография, или ещё что-то. В таких случаях люди вынуждены откупаться.

Существует множество способов, с помощью которых можно получить несанкционированный доступ к аккаунту. Следовательно, вся информация попадёт в руки злоумышленников. Конечно же, лучше этого не допускать, предварительно позаботившись о **защите персональных данных**.

Изучив эту проблему, можно вывести 5 основных рекомендаций по защите персональных данных в социальных сетях:

1. Не следует запускать сомнительные программы, присланные от незнакомого человека, или даже от знакомого (т.к. его страница может быть взломана и находиться в руках злоумышленников).

2. Старайтесь не открывать сомнительные письма от любых адресатов людей, а уж тем более не переходите по ссылкам, которые могут содержаться в этих письмах, так как это могут быть вредоносные ссылки. Например, вы переходите по ссылке, и ваш компьютер автоматически скачивает программу, которая закреплена там злоумышленниками.

3. Проверяйте все скачанные файлы антивирусом, так как в них могут быть помещены специальные вредоносные программы. Например, программа, которая отправляет информацию с вашего компьютера на абсолютно любой другой, в основном на компьютер злоумышленника.

4. При вводе пароля внимательно проверяйте точно ли это настоящая главная страница социальной сети (существуют сайты, которые созданы для того чтобы получать информацию, вводимую пользователем в строки «пароль» и «логин»), например, главная страница «Вконтакте» - https://vk.com. Если, выделяя ссылку, мы увидим лишнюю букву, или хоть какие-то изменения, такие как - https://vkontakte.com, то будьте уверены – этот сайт создан злоумышленниками.

5. При пользовании чужим компьютером следуют помнить, что вся введённая вами информация (пароли, переписки и т.д.) может дублироваться в специальных текстовых документах, не говоря уже о том, что не нужно ставить галочку *запомнить пароли*, а тем более не нужно забывать выходить с социальных сетей, в которых вы авторизовались.

Выполнение всех 5 пунктов позволит улучшить *защиту персональных данных* в социальных сетях. Но самое главное - тщательно всё обдумать, перед тем как оправить письмо, документ, фотографию кому-либо, пусть даже в закрытом от чужих глаз, личном

сообщении. Следует помнить, что при желании можно взломать почти любую страницу в любой социальной сети и все эти данные легко окажутся в руках *киберпреступников*, а что будет дальше, уже описывалось выше. Поэтому следует серьёзно относиться ко всем действиям в Интернете, ведь каждое выполненное вами действие в *мировой паутине* может быть использовано против вас.

Для защиты от внешних интернет угроз необходимо использовать системы предотвращения вторжений на уровне хоста (HIPS). Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации обеспечивают очень высокий уровень. При учете всех мер получаем защиту персональных данных практически от всех типов вредоносного программного обеспечения. В противном случае можно понести огромный ущерб, к которому относятся в том числе и удар по репутации.

Научный руководитель:
доцент, кандидат экономических наук,
доцент кафедры Информационных технологий РЭУ имени Г.В. Плеханова
Хачатурова С.С.

Список литературы:

1. Мамедов Р. Защита персональных данных в социальных сетях. http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/(дата обращения 29.02.2016).
2. Халилов Д. Способы защиты персональных данных в социальных сетях/ URL: http://www.praima.ru/node/351(дата обращения 29.02.2016).
3. Хачатурова С.С. КонсультантПлюс. Справочные правовые системы. М.: Бином. Лаборатория базовых знаний. 2003.
4. Хачатурова С.С. Информационные технологии в юриспруденции (Учебное пособие). Фундаментальные исследования. 2009. № 9. С. 8-9.
5. Хачатурова С.С. Хранение и защита информации. Международный журнал прикладных и фундаментальных исследований. 2016. № 2-1. С.63-65.