УДК 004.056.5

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

М. И. Сухов, О. А. Гнедина
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

Maxx.sukhov@gmail.com
Gnedina61@mail.ru

Рассматриваются основные аспекты безопасности и соблюдение мер предосторожности в социальных сетях. Приведены примеры защиты информации и сохранения конфиденциальности. Приводится ознакомительная настройка параметров безопасности.

Ключевые слова: социальная сеть, конфиденциальность, защита информации, безопасность.

UDC 004.056.5

INFORMATION PROTECTION METHODS IN SOCIAL NETWORKS

M.I. Sukhov, O.A. Gnedina
Don State Technical University, Rostov-on-Don, Russian Federation

Maxx.sukhov@gmail.com
Gnedina61@mail.ru

The paper considers the main aspects of security and compliance with safety measures in social networks. The paper provides examples of information security and confidentiality as well as introductory security parameter settings.

Keywords: social network, privacy, information security, safety.

Введение. Социальные сети занимают важную нишу в жизни современного человека. Людям нравится ними пользоваться, но совсем немногие задумываются о потенциальном вреде, который они могут причинить. Хотелось бы остановиться на некоторых негативных моментах. В частности, через социальные сети происходит доступ к личной информации, то есть обязательно встает проблема несанкционированного доступа. Рассмотрим условия обеспечения конфиденциальности данных на сайтах социальных сетей. По данным социальных опросов, всего порядка 40% пользователей понимают, как ограничить доступ к опубликованной ими информации в социальных сетях. То есть оставшаяся часть аудитории практически беспрепятственно предоставляет доступ к большому объему опубликованной информации, в том числе личного характера.

Сообщая о себе лишние подробности в Интернете, можно опубликовать компрометирующие материалы. Кроме этого злоумышленники могут использовать личные данные чтобы выдать себя за других людей. Кража личных данных в настоящее время настолько распространена, что, по данным статистических исследований, в США она совершается каждые несколько секунд. Настройки параметров конфиденциальности решают проблему лишь отчасти, так как существуют и другие пути утечки личных сведений в общий доступ. Зная, где могут крыться угрозы для конфиденциальности и как их избежать, пользователи, зачастую, могут сами защитить свои данные. В социальных сетях используются сторонние приложения, например, для просмотра гороскопа или проверки IQ. Такие приложения часто запрашивают доступ к личной информации для персонализации работы с ними. Если приложение запрашивает слишком много данных, возможно, его лучше не устанавливать. В социальных сетях также присутствует реклама спонсоров. Компании заключают сделки с социальными сетями, чтобы иметь возможность добавлять спонсорскую рекламу к различным функциям сайта, таким как с пометкой «Нравится».

Чтобы избежать предоставления доступа к слишком большому объему личных данных, следует проверять параметры приложений, контролировать активность приложений в хронике и канале новостей с помощью раздела «Приложения параметров конфиденциальности». Отказаться от спонсорской рекламы нельзя, но можно настроить для нее параметры конфиденциальности. Управление доступом приложений к своим личным данным или их удаление производится с помощью настройки параметров доступа к личной странице. Следует запретить сторонним приложениям доступ к учетной записи в социальных сетях.

Подробные условия. Узнать, какой уровень конфиденциальности обеспечивает социальная сеть, можно, ознакомившись с политикой конфиденциальности. В ней сообщается следующее: какую информацию и каким образом собирает сайт, кто имеет доступ к этой информации, какие меры по обеспечению безопасности реализованы, как долго хранится информация и как можно связаться с администрацией в случае опасений по поводу нарушения конфиденциальности. На большинстве сайтов сведения о политике конфиденциальности размещены в легкодоступных местах. Необходимо регулярно просматривать их, так как политика может измениться в любой момент. Чтобы быстро выявить параметры конфиденциальности, которые могут сделать личную информацию уязвимой к угрозам, можно использовать средство проверки конфиденциальности. При этом не придется знакомиться с подробными условиями, напечатанными мелким шрифтом. Поэтому, после детального ознакомления с политикой конфиденциальности, необходимо настроить параметры в соответствии со своими предпочтениями. В обязательном порядке следует посетить страницу «Политика использования данных» в социальных сетях, чтобы узнать, как можно избежать разглашения личных данных. Однако, следует учитывать, что на некоторых сайтах невозможно запретить раскрытие личных данных.

Когда пользователей помечают тегами в сообщениях, это выглядит безобидно, но и при этом конфиденциальность может пострадать. Контактные пользователи смогут увидеть, что некто помечен тегом в сообщении или на фотографии, даже если у них нет доступа к исходному материалу. Если помечают тегом свое физическое местонахождение, то это также могут отследить все контактные пользователи. Удалить теги или упоминания может быть затруднительно, так как в некоторых социальных сетях нет такой функции. Средства проверки конфиденциальности могут помочь отследить все теги. Следует проверять все теги и упоминания, просматривать записи и фотографии с тегами, прежде чем добавлять их в хронику. Можно удалить теги вручную. Следует одобрить или удалить теги, добавленные к фотографиям, или настроить автоматическое одобрение тегов от определенных контактов. Контакты могут автоматически включать имя пользователя в упоминания и ответы. Однако доступ к таким записям зависит от параметров конфиденциальности контактов. Если настроить учетную запись как «закрытую», то другие пользователи не смогут просматривать записи или отвечать на них без вашего одобрения. Учитывая то, как устроены социальные сети, параметры конфиденциальности друзей непосредственно влияют на нашу конфиденциальность. Если эти параметры недостаточно строги, записи может просматривать множество посторонних людей. Однако даже если установлены строгие параметры, опубликованная информация может распространяться по сети. В некоторых социальных сетях контактным пользователям разрешено копировать и повторно публиковать исходные записи. Посторонние люди могут видеть даже частные записи, если они помечены тегом. Также нужно помнить, что вся информация остается в сети на неопределенный срок, поэтому к опубликованию своих личных данных, фотографий и сообщений надо относиться

аккуратно, а доступ предоставлять только определенному разрешенному кругу лиц. Наличие категории «друзья друзей» означает, что разрешение на просмотр информации могут получить уже совершенно незнакомые люди. Можно делать общедоступным список пользователей, предоставив доступ к их учетным записям широкому кругу лиц. В этом случае учетная запись может быть включена в общедоступный список. Однако, если настроить учетную запись как закрытую, то для подписки на нее пользователям потребуется одобрение хозяина информации.

На некоторых сайтах деактивация учетной записи и ее удаление — это не одно и то же, так что данные учетной записи могут быть очищены не полностью. Бывает так, что каждую учетную запись на одном сайте на конкретного пользователя приходится удалять отдельно. Но деактивация или удаление учетной записи не гарантируют, что все ее следы исчезнут навсегда. Некоторые кэшированные профили или записи могут по-прежнему отображаться в поисковых системах. Информация также может сохраниться на серверах или в базах данных сайта. Поэтому следует ознакомиться, как удалить или отключить свои учетные записи. Деактивированную учетную запись при необходимости можно снова активировать в будущем. Если же удалить учетную запись, вся личная информация, кроме отправленных сообщений, исчезнет навсегда. Удалить учетную запись в некоторых социальных сетях непросто, так как она может быть связана с другими учетными записями. Но при удалении учетной записи будут очищены все контакты, комментарии и записи. Окончательная деактивация учетной записи в каждой социальной сети происходит по-разному, в течении определенного количества времени. Однако, даже после этого, ее содержимое может быть доступно на сайте в течении нескольких дней.

Приведем примеры негативных последствий пребывания в социальных сетях и неаккуратного их использования:

– Немецкая компания Willich уволила своего сотрудника из-за фотографии в социальной сети. Руководителям не понравился снимок, на котором молодой человек несет на руках свою беременную невесту. Официально этот работник уже несколько месяцев числился на больничном с межпозвонковой грыжей. Обманщика рассчитали в тот же день, даже без предварительного уведомления.

– Кадровые агентства уже готовы внести социальные сети в отдельную статью под увольнение. Так, еще четыре года назад, служащая швейцарской страховой компании Nationale Suisse лишилась работы из-за пристрастия к Facebook. Женщина отпросилась с работы, сославшись на мигрень из-за долгого сидения перед компьютером. Но начальство заметило сотрудницу онлайн в Facebook. Ее уволили с формулировкой «утрата доверия компании».

Поэтому следует обращать внимание на собственные действия в социальных сетях и тщательно анализировать весь выкладываемый контент.

Двухфакторная аутентификация. Некоторые социальные сети для улучшения защиты личной информации своих пользователей ввели двухфакторную аутентификацию. Она подразумевает двухэтапный вход в свой личный аккаунт. Первый этап — традиционный — вход с помощью логина и пароля. Второй этап пользователь может выбрать по своему желанию из трёх вариантов. Первый — уникальный код по смс, второй — уникальный список кодов, которые действуют лишь единожды. Третий метод заключается в использовании специальных мобильных приложений, генерирующих коды. К примеру, может использоваться Google Authenticator. Для его настройки необходимо сканировать специальный QR-код с мобильного устройства и ввести специальный код подтверждения. Кроме этого может использоваться токен — компактное

устройство, предназначенное для того, чтобы обеспечить информационную безопасность пользователя. Он используется для идентификации своего владельца и возможности предоставления защищенного удаленного доступа к всевозможным типам информации. Токен находится в собственности пользователя. Самые простые токены не требуют физического подключения к компьютеру. У них имеется дисплей, где отображается число, которое пользователь вводит в систему для осуществления входа. Более сложные подключатся к компьютерам посредством USB или Bluetooth-интерфейсов. Все это может помочь защитить личную информацию от недоброжелателей и обезопасить страницу от взломов.

Выводы. Таким образом, современные пользователи обязаны уделять должное внимание политике конфиденциальности, а также заботится о безопасности своих данных во избежание негативных последствий.