2. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3. *Левшун Д.С., Чечулин А.А., Котенко И.В.* Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. – 2019. – Т. 5. № 4. – С. 114-123.

4. *Куценко А.В., Атутова Н.Д., Зюбина Д.А., Маро Е.А., Филиппов С.Д.* «Алгебраический криптоанализ низкоресурсных шифров Simon и Speck» // ПДМ. Приложение. – 2021. – № 14. – С. 84-91.

5. iKey – Всё для копирования ключей [Электронный ресурс]. – URL: https://ikey.ru/smkey/ (дата обращения 14.10.2022).

6. *Горохов А.В., Гаврин В.А., Мартынов В.А.* Обеспечение информационной безопасности посредством построения комбинированных систем контроля и управления доступом // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – Т.5. №4. – Порядковый номер: 26.

DOI: 10.25728/iccss.2022.61.81.037

Логинова Л.Н., Королев А.Д.

Принципы обеспечения информационной безопасности в социальных сетях

Аннотация: В работе показаны особенности обеспечения информационной безопасности в социальных сетях, проведен анализ существующих способов защиты, даны рекомендации по защите информации и персональных данных.

Ключевые слова: информационная безопасность, утечка данных, защита информации, социальные сети, аутентификация

В настоящее время пользовательские данные представляют высокую ценность для злоумышленников. Так, например, в 2016 году данные более 100 млн пользователей социальной сети «Вконтакте» были выставлены на продажу за 1 биткойн [1]. Данные, которые были утеряны, содержали конфиденциальную информацию, а именно, логины и пароли от социальной сети, имена, номера телефонов.

Важно отметить, что в настоящее время грань между разнообразными интернет-сервисами размылась, сложно произвести категоризацию сервисов, поскольку функционал часто дублируется. Сервисы позволяют общаться, проводить поиск профилей, отправлять и просматривать файлы, заполнять информацию о себе и т.д. Так, например, некоторые мессенджеры полностью повторяют функционал социальных сетей, а настройки безопасности и конфиденциальности идентичны.

Целью работы является проведение анализа обеспечения информационной безопасности (ИБ) социальных сетей, который, в свою очередь, является основой функционирования цифрового пространства современного общества, а также формирования рекомендаций по защите информации и персональных данных пользователям.

Каждый второй человек имеет аккаунт в социальной сети. По данным [2], более 4 миллиардов человек пользуются социальными сетями. Ценность каждого аккаунта зависит от информации, которая в нем содержится, а, в случае массовой утечки, ценность составляет совокупность различных актуальных аккаунтов.

В социальных сетях особо важным объектом является передаваемая информация, поскольку человек по неосторожности может отправить некоторые секретные данные не по зашифрованным каналам связи, а через социальную сеть или мессенджер, а получение злоумышленником доступа к таким данным может иметь весьма серьезные последствия. Так, например, злоумышленник может использовать данные с целью вымогательства, шантажа, получения доступа к финансовым активам.

К сожалению, массовая утечка данных аккаунтов не редкость в текущей мировой ситуации [3]. Под угрозой атаки могут быть и определённые социальные сети, серверы которых базируются в

разных странах и содержат данные большого количества пользователей.

Пользователи социальных сетей не застрахованы от подобных массовых утечек данных, в таком случае вся ответственность ложится на компанию, которая хранит и обрабатывает пользовательские данные, но существуют также и точечные атаки, когда целью злоумышленника является конкретная персона, пользователь, аккаунт, и в таком случае весь риск лежит на конкретном владельце аккаунта.

Точечную атаку стоит расценивать как более опасную для самого пользователя, потому что при такой атаке злоумышленнику необходимо получить доступ к определенному аккаунту с конкретной целью. Цели, как при массовой утечке, так и при точечной атаке, могут быть идентичны, например, получение корпоративных данных, являющихся поводом для шантажа. При защите аккаунта понятия «безопасности» и «приватность» часто не разделяют. Настройки приватности в социальной сети служат для скрытия профиля или отдельных его элементов на площадке и в сети интернет от посторонних глаз. Можно утверждать, что строгие настройки приватности косвенно повышают безопасность аккаунта, но не исключают взлом. В свою очередь, безопасность позволяет предотвратить возможный взлом аккаунта путем более сложной и строгой настройки аутентификации и других параметров доступа к аккаунту.

Обеспечение ИБ в социальных сетях – актуальная проблематика для большого количества компаний, обладающих ценной коммерческой информацией, находящейся в поле поиска злоумышленников.

В исследовании *Verison* [4] указано, что 80 % инцидентов ИБ связано с аутентификацией, методы которой являются средствами обеспечения ИБ в социальных сетях:

- аутентификация по СМС;
- аутентификация только по паролю;
- двухфакторная аутентификация.

Аутентификация по СМС – один из наиболее слабых методов контроля доступа. Аутентификация происходит путем отправки СМС сообщения на указанный мобильный номер с кодом доступа к аккаунту. Уязвимость кроется в возможности перехвата самого

сообщения, а также в системах сотовых операторов, когда, например, можно воссоздать дубликат сим-карты и незаметно перехватывать сообщения. Рекомендуется отказаться от такого способа аутентификации, а в случае невозможности не заводить аккаунт или минимизировать обмен любыми данными.

Аутентификация по паролю – это наиболее распространённый способ получения доступа к аккаунту, требующий особого внимания к стойкости пароля и его сохранности. Многие пользователи социальных сетей используют крайне слабые пароли. По данным [5], самыми часто встречающимися паролями стали:

1. «password»;
2. «123456»;
3. «123456789».

Для создания сложного пароля следует использовать случайную комбинацию чисел, заглавных и прописных букв, специальные символы. В работе [6] рекомендуется использовать сложные, уникальные пароли длиной больше 8 символов. Важно, чтобы пароль был уникальным и не использовался в других сервисах, т.к. в случае утечки общего пароля от одной социальной сети под угрозой находятся данные в других социальных сетях. Стоит отметить, что использование совершенно разных паролей затруднительно – возникает сложность в запоминании огромного количества случайных паролей. Для облегчения ведения и запоминания пароля от каждой социальной сети можно использовать случайно сгенерированный шаблон пароля с индивидуальным алгоритмом его модификации. Некоторые онлайн-сервисы и социальные сети жестко ограничивают максимальную длину пароля и\или запрещают использовать те или иные специальные символы – это сомнительный подход к обеспечению ИБ платформы, что является причиной задуматься об отказе регистрации в подобных сервисах.

В работах [6, 7] показано, что безопасным и стойким способом аутентификации на сегодняшний день является двухфакторная аутентификация. Двухфакторная аутентификация позволяет избежать несанкционированный взлом системы или аккаунта, снизить риск утечки персональных данных и другой важной информации в корпоративных сетях, а также обезопасить пользователя от ошибочных транзакций в интернет-магазинах, социальных сетях и т.д. [7].

Большинство современных социальных сетей позволяют следить за входами и попытками входа в аккаунт, а также просматривать, на каких устройствах, с каких IP-адресов выполнен вход, уничтожать текущие сессии. Следует отметить, что неизвестная попытка входа в аккаунт является весомым поводом сменить пароль, проверить личные онлайн-сервисы. В случае, если личный аккаунт в социальной сети не нужен, то рекомендуется удалить всю личную информацию и аккаунт.

Важным аспектом ИБ в социальных сетях являются настройки приватности, рекомендуется использовать максимально строгие правила: ограничивать видимость номера телефона, подробной информации о личности, фотографиях и другой информации, которой может воспользоваться злоумышленник. Рекомендуется регулярно проверять настройки приватности, с осторожностью относиться к любым сообщениям от незнакомых людей, не открывать подозрительные файлы.

В последнее время появилась возможность использовать аккаунт в социальной сети для входа в другие сервисы в интернете, однако стоит учесть, что это небезопасный метод входа, т.к. предоставляется сторонним сервисам информация об аккаунте и его владельце, а в случае взлома аккаунта в социальной сети злоумышленник получит доступ ко всем сервисам, где была выполнена аутентификация.

Проведенный анализ методов и способов защиты информации и персональных данных в социальных сетях позволяет сформулировать следующие рекомендации: не следует оставлять социальные страницы в сетях заброшенными, и в случае их неиспользования – важно удалять профиль и личные данные аккаунта; не следует принимать заявки от неизвестных аккаунтов, поскольку те могут быть использованы для кражи личных данных пользователя; рекомендуется использование сложных паролей; рекомендуется настроить двухфакторную аутентификацию при входе на страницу в социальной сети; не следует делиться конфиденциальной информацией и важно ознакомиться со всеми пунктами пользовательского соглашения, поскольку многие социальные сети, как владельцы аккаунтов, имеют право продавать личные данные третьим лицам-сторонам.

В настоящее время, когда утечка данных, паролей и другой конфиденциальной информации не редкость, следует максимально

ответственно подходить к ИБ в социальных сетях, использовать двухфакторную аутентификацию, а также регулярно изменять пароли, интересоваться новостями в сфере безопасности, а при выявлении утечки заранее обновлять пароли и доступы к социальным сетям.

Литература:

1. Данные более 100 млн аккаунтов «Вконтакте» продаются в сети за 1 биткоин. – URL: https://habr.com/ru/company/bitrix/blog/305704/ (дата обращения 03.10.2022).

2. Статистика социальных сетей на 2021 год. – URL: https://logotip.online/blog/statistika-socialnyh-setej/ (дата обращения 03.10.2022).

3. Безопасность в социальных сетях. – URL: https://vc.ru/social/81702-bezopasnost-v-socialnyh-setyah (дата обращения 03.10.2022).

4. Двухфакторная аутентификация. Уже пора? – URL: https://www.securitylab.ru/blog/personal/sborisov/347776.php (дата обращения 04.10.2022).

5. Анализ паролей из утечек 2020-2021 года по версии LeakCheck. – URL://www.securitylab.ru/blog/company/leakcheck/351426.php (дата обращения 05.10.2022).

6. *Лим В.Б.* Создание надежных паролей // Проблемы науки. – 2021. – №3 (62). – URL: https://cyberleninka.ru/article/n/sozdanie-nadezhnyh-paroley (дата обращения 11.09.2022).

7. *Замолоцких В.С., Сидоренко В.Г.* Разработка методики восстановления данных на запоминающих // Надежность. – 2022. – Т. 22. № 1. – С. 56-62. DOI: 10.21683/1729-2646-2022-22-1-56-62