Е. Г. Кондратова

СОЦИАЛЬНЫЕ СЕТИ И КОРПОРАТИВНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Развитие человечества не стоит на месте. Разрабатываются и создаются новые товары и новые технологии, чтобы облегчить и упростить нашу жизнь, особенно если это касается бизнеса и общения.

С развитием Глобальной сети Интернет появилось множество вариантов решения любых задач в любых сферах деятельности, это не только удобный способ получения информации, но и важный инструмент для общения. Так, стали появляться различные средства социальных сервисов Интернета, начиная с привычной для нас электронной почты и заканчивая социальными сетями, форумами и блогами.

В мире современных технологий наиболее успешно развиваются социальные сети, направленные на построение в Интернете сообществ людей со схожими интересами, деятельностью, взглядами на те или иные события. Поэтому, как и любой другой ресурс сети Интернет, социальные сети имеют не только достоинства, но и недостатки, которые влияют как на отдельных лиц, так и на общество в целом.

На сегодняшний день в России порталы социальных сетей содержат персональные данные миллионов пользователей, тем самым обеспечивая возможность разнообразного общения между участниками и поиска друг друга на портале и представляя собой огромные онлайн-директории, которые при желании доступны каждому.

Таким образом, возникает ряд вопросов, касающихся обеспечения информационной безопасности (ИБ) данных ресурсов и правового регулирования отношений в области соблюдения законодательства РФ.

Важнейшая задача в деле обеспечения информационной безопасности России — осуществление комплексного учета интересов личности, общества и государства в данной сфере. Доктрина ИБ РФ эти интересы определяет следующим образом:

1. Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;

2. Интересы общества в информационной сфере заключаются в обеспечении интересов общества в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;

3. Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека (гражданина) в области получения информации. Одновременно требуется использование этой сферы только в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, безусловного обеспечения законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование различных форм общественного контроля над деятельностью федеральных органов государственной власти и органов государственной власти

субъектов РФ. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности [1].

Данная иерархия затрагивает различные сферы деятельности человека, в том числе его пребывание в социальных сетях, так как для многих людей это стало незаменимым источником общения, новостей, развлечения, отдыха. Также следует отметить, что каждая ступень иерархии «человек — организация — государство» может так или иначе воздействовать на всю цепочку в целом и являться мощным рычагом как для манипулирования конкретными людьми, так и для разжигания скандалов национального характера. В работе рассмотрена «золотая середина» вышеизложенной иерархии, а именно использование социальных сетей в организации со стандартной архитектурой сети и системными характеристиками при использовании сервисов социальной сети.

Как показывает статистика компании ЗАО «Лаборатория Касперского» [2], с каждым годом растет количество фишинговых атак и спама именно в социальных сетях, которые пока остаются бесспорным лидером среди общеизвестных источников коммуникации. Поэтому работодателям стоит задуматься о защите своих данных и данных организации, а также об осведомленности сотрудников о безопасной работе в социальных сетях и о внедрении и усилении мер обеспечения защиты информации в плане предотвращения ее утечки, защиты репутации, сохранения коммерческой тайны.

Повышенный интерес к сервису социальных сетей находит отражение в деятельности компаний и имеет двойственную природу. С одной стороны, чаще всего в крупных компаниях очень строго относятся к работе сотрудников, простоям и потере денег из-за некачественного выполнения ими своих обязанностей, результатом чего является блокировка выхода на развлекательные сайты, с том числе сайты данной категории. Такой запрет использования социальных сетей на рабочем месте, в свою очередь, приводит к тому, что сотрудники прибегают к помощи непроверенных продуктов, скачанных на мошеннических сайтах, переходят по непроверенным ссылкам, тем самым увеличивая риск потери данных. С другой стороны, возможность компании получать более подробную и систематизированную информацию о сотрудниках, партнерах и клиентах растет по мере расширения использования социальных сетей. Следует отметить, что подобные сервисы широко применяются продвинутыми сотрудниками для поиска необходимых контактов и выхода на нужных людей, минуя бюрократический аппарат и социальные барьеры.

Несмотря на вышеописанные проблемы, большинство компаний не задумывается о потенциальной возможности утечки информации посредством социальных сетей, а обращает внимание на потерю рабочего времени сотрудниками и снижение производительности, что также является заблуждением. Существует немало других факторов, которые снижают производительность работы сотрудников, например, сотрудник зашел в соседний отдел и заговорился с коллегами, пропустив важный звонок, вследствие чего компания потеряла значительную прибыль, в то время как он мог обсудить тот же вопрос в сети, онлайн, находясь на своем рабочем месте рядом с телефоном.

Можно выделить некоторое количество потенциальных угроз, связанных с возможными потерями для компании. Предотвращение данных угроз является неотъемлемой частью общих стратегий построения систем управления информационной безопасностью, таких как политика ИБ организации, анализ и оценка рисков ИБ, поэтому для защиты от утечки данных стоит рассматривать такие угрозы наряду с другими актуальными угрозами ИБ.

Самый простой пример угрозы утечки данных: сотрудник компании, пользуясь социальной сетью, меняет статус, который каким-то образом компрометирует организацию, например, раскрывает конфиденциальную информацию, которая еще не была пущена в канал вещания или рассылку. Подобного рода действия могут носить как случайный, так и умышленный характер. Ярким

примером причины умышленного действия могут служить массовые забастовки, сокращения, когда недовольство некоторой группы людей может вызвать массовые рассылки различной информации, грозящей репутации компании посредством клеветы. Стоит отметить, что владельцы социальной сети не несут ответственности за персональные данные пользователя, а также за распространение и удаление размещенной информации, что указано в пользовательском соглашении. Соответственно, действие Федерального закона «О персональных данных» не распространяется на нее. Поэтому следует четко понимать, что вся ответственность лежит на пользователях интернет-ресурса.

Другой непредсказуемой угрозой ИБ компании является собранная инсайдером совокупность данных о конкретном пользователе (человеке) с нескольких ресурсов с целью построения полного портрета: образование, карьера, интересы, семья, личные данные и другое. При этом подопытный становится персонализированной целью злонамеренных действий, в то время как для работодателя возрастает риск целевых атак. Хорошим примером является использование злоумышленником социальной инженерии.

Еще один яркий пример — это халатное использование социальных сетей большинством пользователей. Ведь люди сами добровольно выкладывают информацию о себе, об учреждениях, в которых они работают, что чаще вредно сказывается на самих пользователях. Например, социальные сети могут легко использоваться работодателями для проверки сотрудников, при этом профиль пользователя может сыграть как положительную, так и отрицательную роль.

Но самой актуальной угрозой использования социальных сетей была и остается возможность заражения вирусами. Большинство рассматриваемых сервисов используют огромное количество приложений и дополнительных ресурсов для привлечения и заинтересованности участников — музыка, видео, фотографии, изображения, что требует от пользователя установки дополнительного ПО или плагина для ПО. Тем самым под видом безобидного приложения скачивается вирус, троянская программа, шпион или делается переадресация на идентичный сервис с целью выявления аутентификационной информации.

Для корпоративной ИБ основными мерами защиты от утечки данных являются организационные меры, начинающиеся с построения системы управления ИБ, анализа и оценки рисков, выявления наиболее ценной информации и активов, с последующим моделированием убытков, вызванных утечкой информации, а также выявлением и разработкой оптимальных мер по защите. Существует ряд таких мер, например инженерно-технические меры защиты — комплексные средства мониторинга, анализа и фильтрации входящего и исходящего трафика на уровне шлюзов, а также средства анализа поведения приложений и сетевых коммуникаций. Или организационные меры — управление доступом к потенциально опасной среде, то есть диверсифицированные внутрикорпоративные политики «белых списков» и фильтрации контента для различных групп пользователей [3]. Еще одним важным аспектом является работа с человеческим фактором в направлении усиления рабочей дисциплины, корпоративной этики, а также донесение до сотрудников понимания, что политики ИБ служат не для вторжения в их частную жизнь и ущемления достоинств или прав, а являются мерой предотвращения потерь и утечки данных компании, особенно если речь идет об информации ограниченного доступа. Следует проводить такие мероприятия, как тренинги и обучение персонала, в том числе риторика и деловое общение, что демонстрирует заинтересованность работодателя в повышении мер защиты информации.

Стоит еще раз отметить, что проблемы утечки информации грозят репутации компании, причем доверие клиентов для большинства из них, как показывает практика, равносильно деньгам. Неважно, каким образом компания решает взаимодействовать с таким явлением, как социальная сеть, важно, чтобы была разработана стратегия решения проблем утечки данных и политика ИБ компании.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации.
2. Аналитика фишинговых атак. URL: http://www.securelist.com/ru/analysis (дата обращения: 23.01.2013).
3. Журнал «Information Security/ Информационная безопасность». URL: http://www.itsec.ru (дата обращения: 02.02.2013).
4. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. *Губанов Д. А., Новиков Д. А., Чхартишвили А. Г.* Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д. А. Новикова. М.: Издательство физико-математической литературы, 2010. — 228 с.