обеспечение дальнейшего быстрого и беспрепятственного управления им. Так, постепенно разрушая сознания отдельных индивидов можно добиться разрушения целой нации, последствия которого будут катастрофическими.

Таким образом, в связи с глобальным распространением и постоянным развитием новых форм информационно-коммуникационных технологий все сложнее обеспечивать защиту персональных данных от несанкционированного доступа и ее противоправного использования. Для минимизации вероятности утечки информации необходимо не разглашать личные данные третьим лицам, не использовать социальные сети в качестве средства связи, а также не хранить персональную информацию в смартфоне, ноутбуке и иных гаджетах без использования средств защиты данной информации.

УДК 004.056

СОЦИАЛЬНАЯ СЕТЬ КАК ИСТОЧНИК ИНФОРМАЦИИ О ЛИЧНОСТИ

Шурко В.В., студентка 4-го курса
Научный руководитель – Солодовников С.Ю., д-р. экон. наук, профессор

Белорусский национальный технический университет
г. Минск, Беларусь

Быстрое развитие информационных технологий способствует появлению новых средств передачи и обмена информацией. Межличностное общение происходит через мобильные приложения или в социальных сетях, позволяющие передать не только личную информацию, но и решать деловые вопросы. Поскольку регистрация в социальных сетях требует ввода личных данных, то изначально мы предоставляем персональную информацию о себе каждому, кто захочет идентифицировать нашу личность. К тому же удаление отдельной информации или профиля в целом не означает бесследного исчезновения информации и невозможности восстановить данные.

Существуют некоторые способы защиты личных данных. Почти все социальные сети имеют правила разграничения доступа различных категорий пользователей к информации, содержащейся на странице пользователя. Например, можно дать доступ к одному из своих альбомов всем пользователям, а к другому – только друзьям. К общим механизмам безопасности, не привязанным к социальным сетям, например, относится использование защищенного протокола взаимодействия с Web-серверами. То есть при входе и пребывании в социальной сети должен использоваться протокол https. Также не рекомендуется добавлять незнакомых людей в друзья, вступать в подозрительные группы, устанавливать неизвестные приложения [1].

Так, говорить о конфиденциальности личной информации не приходится, поскольку мы сами оставляем ее в свободном доступе в различных источниках, в том числе социальных сетях. Однако, при необходимости скрытия персональных данных можно использовать следующие средства защиты информации: ограничивать доступ к личной информации, использовать защищенный протокол взаимодействия с Web-серверами и не совершать действия, которые могут привести к утечке информации.

Литература

1. Защита персональных данных в социальных сетях [Электронный ресурс]. Режим доступа: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/. Дата доступа: 25.02.2017.