ПОД-СЕКЦИЯ 3. Информатика, вычислительная техника и автоматизация

Михайлов Д.В.
к.т.н., доцент кафедры
Охраны труда и безопасности жизнедеятельности
Игнатенко А.А.
студентка факультета
Инновационной экономики и кибернетики
Восточноукраинский национальный университет
имени Владимира Даля, г. Луганск

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

В последнее время одной из самых актуальных тем для дискуссий является так называемое «поглощение» пользователей интернетом социальными сетями. Влияние этих информационных систем на жизнь людей огромное. Во всем мире более 80% компаний используют социальные сети в работе. Примерно 78% людей доверяют информации из социальных сетей. Состоянием на сентябрь 2012 года компания «Яндекс.Украина» провела исследование популярности социальных сетей в Украине и опубликовала такие данные: в социальных сетях зарегистрировано более 30 миллионов украинских аккаунтов, лидирует по количеству учётных записей сеть «ВКонтакте» – около 20 млн., на втором месте «Одноклассники» с 6 млн., на «Facebook» зарегистрировано 2 млн. украинцев.

Сегодня социальные сети представляют собой огромные базы данных с самой разнообразной информацией о сотнях миллионов людей по всему миру, кроме того, еще и хорошо структурированной. Социальные сети все больше и больше открываются внешнему миру, и многие личные данные пользователей уже доступны для всех желающих. Чем выше активность человека в социальных сетях, тем больше информации о нем можно собрать совершенно незаметно и легко. Современные социальные сети предлагают пользователям указать практически всю информацию о себе: номер телефона, адрес, фото, видео, интересы, связи, место работы и должность, места отдыха, хобби, любимые книги, личные мысли и т.д. Большую часть информации можно добыть даже без регистрации, остальное – после добавления пользователя в друзья. Вся информация, в том числе и личная переписка, по меньшей мере, доступна администрации сети, никакие настройки не предполагают ее полной приватности. Однако, самое странное, что большинство пользователей предоставляют свою персональную информацию без всякой опаски на то, что она может быть использована кем-то в неблагоприятных целях. В основном это происходит по неопытности пользователей. Последствия халатного отношения с занесением личной информации в социальные сети могут быть самыми непредсказуемыми и трагичными. Самым безобидным вариантом использования личных данных без разрешения пользователя являются внутренние механизмы социальных сетей для подбора потенциальных знакомых, показа таргетированной рекламы или отбора потенциально интересного контента. Эти процессы стали почти стандартом в большинстве социальных сетей.

Больше проблем пользователям приносит утечка личных данных по

вине сети. Это неоднократно наблюдается в разных проектах. Примером такой утечки данных может служить одна из самых больших по размерам утечка личных данных 77 млн. пользователей, произошедшая в апреле 2011 года в игровой сети «PlayStation Network». Еще одним примером утечки информации может служить случай, произошедший летом 2012 года в социальной сети «LinkedIn». Одному из пользователей удалось украсть базу данных пользователей сети. Такие случаи не единичные и большинство из них скрывается от общественности.

Еще более серьезной проблемой безопасности информации в социальных сетях является взлом отдельных аккаунтов и получение доступа ко всей личной информации отдельного пользователя. Сегодня совершить взлом аккаунта не составит труда даже обыденному пользователю, достаточно уметь пользоваться социальной инженерией. В большинстве случаев пароль – единственная защита данных пользователя социальной сети от других пользователей или недоброжелателей.

Существует определенная категория вирусов, которые высылают своим создателям данные аккаунта пользователя, на компьютере которого они сейчас находятся. Самый эффективный и простой способ похитить информацию из аккаунта пользователя, это создание фальшивой страницы, или фишерского сайта. Спамер посылает пользователю социальной сети электронное письмо якобы от имени администрации социальной сети, либо ее пользователя. В письме может содержаться приглашение стать другом или посмотреть интересное видео. В сообщении будет указана ссылка, ведущая на фальшивую страницу, где необходимо указать свои логин и пароль, после чего эти данные будут доступны спамеру. Примером фишинга может служить инцидент в социальной сети «Twitter», когда в начале ноября 2012 года фишинговый сайт, якобы от имени самого «Twitter», разослал письма с просьбой сменить пароли, перейдя для этого по указанной ссылке.

Проблемой является и то, что доступ к личной информации пользователей имеется у достаточно большой группы людей. Во-первых, это сотрудники социальной сети. Во-вторых, сотрудники правоохранительных органов: ФСБ в России или ЦРУ в США. Основатель «Wikileaks» Джулиан Ассандж заявляет, что у «Facebook» имеется специальный интерфейс для разведки США. В России же популярной социальной сетью «ВКонтакте» публично были признаны факты сотрудничества с правоохранительными органами и передачи им личных данных пользователей сети.

Многие пользователи социальных сетей сейчас начинают задумываться о безопасности их информации. Некоторые даже вовсе удаляют свои страницы из сетей, однако удаление не дает гарантии, что информация удалена полностью; часто информация еще долго хранится на серверах социальных сетей и может быть использована злоумышленниками.