Секция «Глобальная безопасность»

Социальные сети как пространство информационных угроз

Научный руководитель – Меньшенина Наталья Николаевна

Бобылева Мария Олеговна
Студент (бакалавр)
Уральский федеральный университет имени первого Президента России Б.Н.Ельцина, Екатеринбург, Россия
E-mail: bobileva.maria086@yandex.ru

Социальные сети как пространство информационных угроз
Бобылева Мария Олеговна
студентка 4 курса
Уральский Федеральный университет им. первого президента России Б.Н.Ельцина
Безопасность инфраструктур и территорий в системе государственного и муниципального управления, Екатеринбург, Россия
mailto:bobileva.maria086@yandex.ru

В современном мире происходят постоянные изменения в геополитической ситуации, создавая все новые угрозы национальной безопасности государств. Национальная безопасность - состояние защищенности личности, общества, государства от внутренних и внешних угроз. Одной из составляющей национальной безопасности является проблема обеспечения безопасности в социальных сетях.[1]

На сегодняшний день Россия является страной с наиболее высокими показателями активности граждан в социальных сетях. По результатам исследования http://www.comscore.com/, онлайновая аудитория в России увлечена социальными сетями больше, чем кто-либо в мире. Согласно данному исследованию в России проводят в социальных сетях в среднем по 6,6 часов, на втором месте находится Бразилия 6,3, пятёрку лидеров завершает Испания, на последнем месте находится Италия - 3,2 часа.[2]

Самыми популярными социальными сетями в России являются: ВКонтакте - 12 млн. пользователей ежедневно; Одноклассники - 7,2; Мой мир - 5,3; Facebook-1,2, так же популярность набирают Instagram, Google+ и многие другие.[3]

Увеличение количества исследований о проблеме безопасности в социальных сетях социальных сетей позволяет сделать вывод, что данная тема является актуальной.

По результатам исследования компании Омнибус GfK, с 2008 года по конец 2015 количество пользователей социальными сетями выросло с 25,4% до 70%, это показывает насколько население вовлечено в пространство «Интернет» и насколько важно следить за безопасностью и пресекать мошенничество.[4]

Доверяя соцсетям, люди со всех уголков планеты размещают личную информацию, фотографии, информацию о финансах и здоровье, геолокации и многое другое. Совершая все вышеперечисленные действия, они не всегда информированы о потенциальных угрозах. Для предотвращения мошенничества и предупреждения населения, необходимо исследовать характер угроз и защиты от них.

Российские граждане - пользователи социальных сетей оказываются уязвимыми в общении в социальных сетях и распространении конфиденциальной личной информации в пространстве «Интернет».

Одной из распространенных угроз в социальных сетях выступает - специфическим образом понимаемая, социальная инженерия как метод получения информации.[5]

Основной целью мошенников является получение информации о паролях, банковских данных и других защищенных системах, например для шпионажа и сбора информации о сотрудниках различных компании.

Одним из методов сбора информации, является создание мошенниками «фейковых» страниц. Благодаря общению с выбранной жертвой через эти страницы злоумышленники добывают конфиденциальную информацию. Часто таких новых «друзей» интересуют не только любимый цвет и музыка, а и место работы, корпоративная культура, руководство. Эта информация может быть использована во вред человеку, организации, компании.

Еще одной не менее важной угрозой для пользователей социальных сетей является фишинг. Фишинг- это вид интернет мошенничества с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей - логинам и паролям. С помощью спама, почтовых и мгновенных сообщений они выманивают у пользователей эту информацию, например, это могут быть номера банковских карт, пароли, банковские счета.[6]

Размещение ссылок на «стене», наряду с вышеперечисленными, так же несет потенциал угроз. «Стена» в социальной сети представляет собой социальный портал, через который можно легко распространять различные вредоносные программы. В свою очередь данные программы могут добыть информации не только о пользователе данным ПК, но и попасть в корпоративную сеть, если пользователь сидит в социальной сети в рабочее время.

Самым популярным способом является распространение вредоносных ссылок на «стене» пользователя. Под видом различных видео, картинок, фотографий и много другого злоумышленник распространяет ссылки. После перехода на такого рода ссылки гарантирует открытие совсем других сайтов, с мгновенной загрузкой на ПК вирусов, которые ориентированы на кражу конфиденциальной информации.

В последнее время набирает популярность общение пользователей через приложения-мессенджеры такие как: Skype (раскрывает IP-адреса своих пользователей); Telegram (сомнительная система end-to-end шифрования); ICQ (принадлежит Mail.ru - легко уязвим для силовиков); Viber,Whats app, Face time, iMessage - легко взломать, это еще раз доказывает уязвимость пользователей. Данные приложения и их системы безопасности выбраны нами как тема дальнейшего исследования.

Таким образом, пользователи интернета сталкиваются с проблемой обусловленной с одной стороны, информированностью и знаниями мошенников а с другой, недостатком информированности со стороны пользователей. Именно поэтому проблема вызывает интерес как теоретиков, так и практиков в области социальных коммуникаций. По нашему мнению, информирование пользователей социальных сетей о потенциальных угрозах снижает риск для российских пользователей и, в целом, способствует нейтрализации названных угроз.

Источники и литература

1) Бобылева М.О., Янковская Я.А.Национальная безопасность России и социальное самочувствие граждан: некоторые аспекты проблемы//Сборник статей Международный научно-практической конференции.2016.ч3.С.184-185.

2) В России сидят в социальных сетях больше всего в мире. URL: http://mediarevolution.ru/audience/behavior/2068.html

3) Free Social Media Statistics. URL:http://www.socialbakers.com/statistics/
4) Количество пользователей интернета в России. URL: http://www.bizhit.ru/index/users_count/0-151
5) Социальная инженерия как метод добычи информации. URL: http://it-sektor.ru/sotscial-naya-inzheneriya-kak-metod-dobychi-informatscii.html
6) Фишинговая атака. URL: http://it-web-log.ru/2012/02/fishingovaya-ataka/