Секция «Глобальная безопасность»

Социальные сети как фактор стратегической безопасности

Толстова Екатерина Григорьевна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет глобальных процессов, Направление глобальной экономики и управления, Москва, Россия
E-mail: butenko.f17@gmail.com

Сегодня социальные сети стали неотъемлемой частью нашей жизни, а также немаловажным фактором в установлении и поддержании хороших отношений на разных континентах и в разных странах. Социальные сети оказались полезными для людей, которые разделяют одни и те же интересы в профессиональном плане, с точки зрения различных исследований, в случайном социальном общении и т.д. Также они сыграли большое значение для многих компаний и холдингов, которые использовали социальную сеть для продвижения своих маркетинговых стратегий и IT. Благодаря социальным сетям такие компании впоследствии оказались прибыльными.

Однако, как и любой другой веб-сайт или приложение, социальные сети привлекают большой приток пользователей, а потому безопасность личной информации пользователей в социальных сетях подвергалась различным угрозам безопасности.

Сразу стоит внести ясность в понятийный аппарат таких определений как «стратегическая безопасность» и «стратегическая безопасность в социальных сетях». Так, стратегическая безопасность - это «конвергенция двух концепций (стратегической стабильности и безопасности во всех аспектах)», а стратегическая безопасность в социальных сетях - это «защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователем информации».

Сайты социальных сетей (SNS) - это типы сайтов Web 2.0, которые позволяют пользователям создавать онлайн-аккаунты, которые отображают их профили.

SNS - это группа веб-сайтов, которые предоставляют людям создать онлайн-профиль и поделиться этим профилем с другими. Её также можно определить как веб-сервис, который позволяет отдельным пользователям создавать общедоступный или полуобщественный профиль в ограниченной системе, составлять список других пользователей в системе, к которым они имеют общее подключение, и просматривать список подключений, сделанных другими пользователями в системе.

Наиболее популярными сайтами Web 2.0 считаются следующие SNS: Facebook, Twitter, MySpace и LinkedIn, Instagram, Telegram, Tik-Tok. Эти социальные сети предоставляют пользователям платформу для создания и поддержания отношений из разных точек мира в любом её проявлении (будь то смс, аудио или видеоролик). Большинство из этих SNS специализированы и посвящены определенным сферам жизни, включая образование, религию, работу, а также различные развлекательные платформы.

SNS сочетает в себе различные функциональные возможности, которые надолго привязывают к ним своих пользователей. Компании и учреждения, в настоящее время, стремятся разработать политику, которая будет использоваться для контроля их работников или студентов за количеством времени, которое они проводят в Интернете, отвлекаясь от работы.

Пользователи SNS всегда были введены в заблуждение прозрачной анонимностью, которой они пользуются в желаемой социальной сети. Однако следует отметить, что ничто,

содержащееся в профиле пользователя, не защищено. Различные организации также используют социальные сети для продвижения интересов своей компании. Социальные сети создают некоторые проблемы безопасности для организаций и холдингов. Некоторые из этих проблем безопасности включают споры об ограниченной пропускной способности сети со стороны сотрудников, использующих ее для целей SNS; вредоносная атака и непреднамеренное разглашение конфиденциальной информации.

Основываясь на угрозах безопасности, с которыми сталкиваются пользователи сайтов социальных сетей, основное внимание уделяется решению некоторых основных проблем безопасности, которые могут отрицательно сказаться на том или ином пользователе, чтобы бороться с ними или смягчать их. Эти решения по безопасности используются для обеспечения аутентификации пользователей, а также поддержания конфиденциальности и целостности информации в SNS.

Далее, хотелось бы выделить такую категорию опасности в SNS - это деанонимизация. Анонимизация в социальной сети позволяет пользователям скрывать информацию, которая может подорвать их конфиденциальность. Такая информация может включать их имена, фотографии, адреса и другие конфиденциальные данные. Причина такой анонимности заключается в обеспечении защиты пользователя от рекламодателей, разработчиков приложений и исследователей интеллектуального анализа данных, которые будут нарушать конфиденциальность пользователей. Тем не менее, были проведены некоторые исследования, которые доказали, что такая деанонимизация пользователей онлайн-социальных сетей возможна. Деанонимизация позволяет злоумышленникам использовать общедоступные записи, такие как данные о браке и рождении. Комбинация информации о человеке может быть получена из некоторых социальных сетей в качестве основы для деанонимизации пользователя. Таким образом, атака с целью деанонимизации стала еще одной угрозой для пользователей, используемой злоумышленниками в обход настроек конфиденциальности пользователя.

В основном, подход к решению проблемы безопасности можно разделить на три категории:

- конфиденциальность информации / данных;
- целостность;
- аутентификация.

Конфиденциальность — это гарантия для объекта (данных или информации), что никто не сможет прочитать или получить к нему доступ, кроме получателя, который явно указан отправителем.

Целостность (данных или информации) подразумевает, что у того ил иного объекта есть уверенность в том, что в нем не было произведено никаких изменений ни намеренно, ни непреднамеренно.

И, наконец, аутентификация - это гарантия для объекта (системы данных или информации), что другой объект (который может быть пользователем, агентом или средством доступа) является тем, за кого он себя выдает.

Таким образом, сайты социальных сетей становятся очень полезными среди людей разных областей и профессий. Студенты колледжей и высших учебных заведений используют популярные сайты социальных сетей в качестве средства коммуникации. Предприятия, холдинги и организации также используют социальные сети для продвижения деловых интересов и создания имиджа сотрудничества. Таким образом, в данном параграфе были обсуждены основные проблемы безопасности, которые широко распространены в большинстве социальных сетей. Были предложены два подхода к смягчению некоторых проблем конфиденциальности, которые могут породить за собой более серьезные проблемы.

Источники и литература

1) Кокошин А.А. Политико-военные и военно-стратегические проблемы национальной безопасности России и международной безопасности. М.: Высшая школа экономики, 2013.
2) Кулагин В.М. Международная безопасность. М.: Аспект Пресс, 2007. - С. 23-37.
3) Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004. С. 13.
4) Панарин С.А. Безопасность как ценность и норма: опыт разных эпох и культур. СПб: Интерсоцис, 2012.
5) Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.
6) Шаньгин В.Ф. Информационная безопасность и защита информации. — М.: ДМК, 2017. — 702 с.