Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Интенсивность информационного обмена, сложность современных алгоритмов обработки информации, разнообразие угроз и средств защиты от них обусловливают необходимость применения разнообразных автоматизированных средств и систем для решения задач обеспечения информационной безопасности.

Одним из современных подходов к решению задач защиты информации информационных систем является внедрение SIEM-технологии. Основной функцией SIEM-систем является анализ информации, поступающей от разных источников. На основе анализа данных из этих источников выявляются отклонения от нормального функционирования, заданного критериями безопасности, и в случае обнаружения происходит оповещение администратора безопасности.

SIEM-система используется для: анализа информации, поступающей от различных источников; предоставления доказательной базы при расследовании инцидентов информационной безопасности; предоставления структурированной информации, необходимой при аудите информационной безопасности; обеспечения непрерывности работы сервисов путем обнаружения сбоев в их работе; структуризации информационно-телекоммуникационной системы.

SIEM-система выявляет следующие события и инциденты информационной безопасности: сетевые атаки во внутреннем и внешнем периметрах; вирусные эпидемии или отдельные вирусные заражения; попытки несанкционированного доступа к информации ограниченного распространения; мошенничества; ошибки и сбои в работе информационных систем; уязвимости; ошибки конфигурации в средствах защиты и информационных системах; целевые атаки.

Основными задачами обеспечения информационной безопасности, которые ставятся перед SIEM-системой, как правило, являются следующие:

централизованное хранение журналов событий;

обработка и корреляция событий;

оповещение об инцидентах; расследование инцидентов; управление инцидентами (инцидент-менеджмент).

Результат применения SIEM-систем:

повышение уровня защищенности информационной инфраструктуры за счет оперативной реакции на инциденты информационной безопаснсоти;

ускорение и автоматизация процесса идентификации и последующего расследования инцидентов;

централизованный подход к задачам обработки и хранения событий информационной безопасности.

Благодаря использованию SIEM-систем значительно снижается время реагирование на атаки, а, следовательно, и экономические затраты на восстановление системы.

ИДЕНТИФИКАЦИЯ УЧАСТНИКОВ СОЦИАЛЬНОЙ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.А. ИВАНОВА, А.В. КОБЗАРЬ

ФГБОУ ВО «Московский технологический университет»

Социальные сети – это многофункциональный сетевой ресурс, который привлекает к себе всё больше внимания самых разных структур, поскольку охватывает огромную аудиторию пользователей и имеет большую долю влияния, чем какое-либо другое средство массовой информации. Кроме того, мониторинг социальных сетей позволяет отследить

полную картину общественных настроений, понять, какие проблемы на данный момент являются наиболее острыми и актуальными, что волнует общество в целом и какие идеи вызывают наибольший интерес.

Однако исторически сложилось так, что различные социальные сети имеют совершенно различную целевую аудиторию, а потому необходимо понимать половозрастной состав и активность пользователей каждой конкретной социальной сети [1]. В структуре различных социальных сетей чаще всего преобладают женщины, однако в таких социальных сетях, как LiveJournal и Twitter большая часть активных пользователей – мужчины. Instagram лидирует по количеству активных пользователей — около 86,7% аудитории Instagram публикуют сообщения не реже одного раза в месяц, аудитория Вконтакте также весьма активна — около 40,3%, доля активных пользователей Twitter составляет 13,4%, наименее активными являются пользователи социальной сети LiveJournal (всего 0,7% аудитории). Следует отметить, что наиболее активными пользователями социальных сетей являются люди в возрасте от 18 до 44 лет, причём молодая аудитория (от 18 до 34 лет) наиболее часто встречается Вконтакте и Живом Журнале, в то время как активные пользователи Facebook, Мой Мир и Одноклассники – в основном люди в возрасте от 24 до 54 лет. На этом фоне наблюдается значительное увеличение популярности в России таких социальных сетей, как Instagram и Facebook (в первую очередь в области деловых контактов и бизнеса), и медленно снижается активность российской части Twitter (в том числе и активность спам-ботов).

Многие современные учёные в области социальной психологии, такие как Кац, П. Лазарсфельд, С. Грин, Э.В. Будаев и А.П. Чудинов, В.Д. Нечаев, Щюц, Бергман, Лукман и другие отмечали, что социальная сеть на данный момент представляет собой нечто большее, чем просто средство общения — это целый механизм, имеющий свои закономерности и особенности, мощнейший инструмент воздействия и формирования различных точек зрения [2-6]. И некоторые события, произошедшие за последние 7 лет в мире, свидетельствуют об этом.

Следовательно, социальные сети могут служить индикатором, позволяющим отслеживать развитие политической ситуации.

Террористические организации используют социальные сети для вербовки молодых людей, узнавая через социальные сети подробности об их жизни, взглядах, отношении к власти, "прощупывают" слабые места и начинают психологическую атаку. Таким образом, на данный момент ещё одной важной задачей обеспечения национальной безопасности является своевременное распознавание субъектов-вербовщиков. Соответственно, к вопросам информационной безопасности добавляется проблема идентификации пользователей, ведущих нежелательную деятельность. Учитывая, что социальные сети являются также большими хранилищами информации, сопоставление различных профилей одного и того же пользователя в различных социальных сетях в большинстве случаев позволит сделать вывод о том, что это за человек.

Таким образом, создание системы идентификации решает сразу две крупные задачи:

обнаружение всех сфер влияния злоумышленника и предотвращение его деятельности;

обеспечение быстрого сбора информации о человеке с помощью социальных сетей.

Существующие методы идентификации разбиваются на несколько способов [7]:

первый способ основан на сравнении личной информации пользователя, такой как: логин, имя пользователя, пол, возраст, место жительства, информация о себе и т. д.

второй способ включает в себя сравнение внутреннего наполнения страницы пользователя, т.е. записи, которые он публикует, поскольку нередко один и тот же пользователь публикует одинаковый контент на своих страницах в разных сетях.

третий способ проверяет ссылки на источник, указанный в публикуемых записях. На случай, если пользователь распространяет записи о своей странице в другой социальной сети, чтобы данная информация была доступна всем его друзьям.

четвертый способ подходит для выявления пользователей, тщательно скрывающих свою личность, и основан на принципе ближайшего окружения пользователя: среди друзей пользователя находятся те, кто указал ссылку на свой профиль в другой социальной сети, и уже в указанной социальной сети находятся все общие друзья этих пользователей.

Однако анализ всех составляющих портрета пользователя социальной сети показал, что существующие методы идентификации используют далеко не все возможные ресурсы и не учитывают некоторых особенностей, которые бы позволили однозначно идентифицировать пользователя, как одно физическое лицо.

Список литературы

1 Социальные сети в России, зима 2015-2016 Цифры, тренды, прогнозы[веб-сайт] – URL:https://blog.br-analytics.ru/socialnye-seti-v-rossii-zima-2015-2016-cifry-trendy-prognozy.

2 Щюц А. Структура повседневного мышления // Социологические исследования.

3 Будаев Э. В., Чудинов А. П. Методологические грани политической метафорологии.

4 Kats E., Lasarfeld P. Personal influence. New York : FreePress, 1955

5 Green S. Twitter and Russian protest: memes, networks and mobilization // Центр изучения интернета и общества:[веб-сайт] – URL: http://www.newmediacenter.ru/ru/2012/05/22/твиттер-и-российский-протест-мемы-сет.

6 Бергер П., Лукман Т. Социальное конструирование реальности : трактат по социологии знания. М. : Медиум, 1995. 323 с.

7 Paridhi J., Ponnurangam K., Anupam J. Identifying Users across Multiple Online Social Networks.

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ И КАЧЕСТВА ОЦЕНОК БЕЗОПАСНОСТИ ИТ

Ю.И. ИВАНЧЕНКО

НИИ прикладных проблем математики и информатики БГУ

В окружающем нас мире все большее место занимают ИТ. Каждый из нас вынужден принимать решение использовать ли и насколько использовать их в своей деятельности. И этот выбор основывается на нашем доверии к конкретным ИТ или услугам, предоставляемым с их помощью. Следует особо подчеркнуть, что это доверие должно быть не религиозным, а осознанным, т.е. основанным на знаниях и надежных свидетельствах, качественных оценках.

Вместе с тем, быстрые темпы обновления знаний и, соответственно, изменений технологий и средств информатизации вместе с непрерывно усиливающейся зависимостью бизнеса, обороноспособности, общественной жизни и т.д. от информационных технологий, объективно не позволяют своевременно получить такие свидетельства, которые позволяли бы сформировать осознанный приемлемый уровень доверия.

Современная воспитательно-образовательная парадигма (деградация классического образования) не оставляет надежды на улучшение ситуации в части обретения