Тип работы: Отчет по практике

Предмет: Информационные системы и процессы

СОДЕРЖАНИЕ

Введение

Одной из актуальных проблем современной мире является проблема обеспечения безопасности личности, общества, государства в социальных сетях. Немаловажной составной частью этой проблемы является информационная безопасность. По данным зарубежных и российских источников на создание и поддержание высокого уровня безопасности в социальных сетях затрачиваются большие денежные средства. Но с чем же связаны такие затраты? Они связаны с повышенным преступности в социальных сетях. Ведь в соцсетях находится более 60% всего населения мира, где хранятся не только денежные средства, но и конфиденциальная информация. Таким образом, особое внимание в защите информационной безопасности необходимо пристальное внимание на социальные сети.

1. Особенности информационной безопасности в социальных сетях

1.1 Статистика атак на web-сервисы

На основании статистики от positive technologies [1] являющейся одной из ведущей российской компании в области кибербезопасности определила увеличение атак на веб-сервисы за 1 квартал 2022 года, так на рисунке 1 представлена сводная характеристика по количеству атак за 2021-2022 год.

Как можно заметить из рисунка 1 за 2021 год было совершено более 2000 тысяч атак на веб-сервисы, где хранятся персональные данные людей. Последствиями таких атак является утечка конфиденциальной информации, а также приводят к сбоям работы организации и сервисов, на рисунке 2 представлены основные жертвы хакерский атак, а также данные, которые были украдены у компаний.[1]

Из рисунка 2 можно заметить, что из-за ненадлежащей защиты веб-сервисов страдают в большей степени частые лица, так на них приходится большая часть потери конфиденциальной информации, а также финансовые потери.

1.2 Опасности в социальных сетях

Помимо злоумышленников, которые хотят завладеть вашей информации, существуют и другие опасности к ним относятся:
1) Проблема конфиденциальности. Размещая информацию о себе в социальных медиа, вы должны быть готовы к тому, что ее может увидеть большое количество людей. В итоге, ваша частная жизнь становится достоянием общественности.
2) Хакерство и взлом паролей. Даже если вы принимаете все меры для того, чтобы оградить информацию о

себе от незнакомых вам людей, эти попытки, в конечном итоге, могут оказаться бесполезными. Есть множество хакерских программ, которые помогают подбирать пароли к популярным веб.
3) Виртуальные двойники. Время от времени вы раскрываете информацию о себе: вашу дату рождения, информацию о вашей семье, ваших занятиях, предпочтениях в области литературы и кинематографа, поездках, которые вы совершаете, людях, с которыми вы работаете, месте, где вы живете, и прочая, прочая, прочая. Кто-то может украсть эти данные, собрать их воедино и создать вашего виртуального двойника.

1.3 Виды угроз в социальных сетях

Выше мы выявили основные опасности, которые нас могут поджидать в социальных сетях. Теперь определим какие-же угрозы безопасности существуют в соцсетях.
Под угрозами определяется действие, которое повышает уязвимость к хранимой и обрабатываемой информационный системы, что приводит к ее случайному или предумышленному изменению или уничтожению. Разработаем классификацию угроз в социальных сетях, которое представлено на рисунке 4.

На рисунке видим, что, мошенник представился агентом технической поддержки Вконтакте, после чего просят перейти на по ссылке похожей на ту, которую использует сайт www.vk.com.[4] Как можем заметить помимо социальной инженерии злоумышленник также пользуется угрозой фишинга а именно создают одну ложную страницу сайта, а все переходы со своей страницы перенаправляют на официальный сайт, что снижает подозрения пользователей.
Одним из основных способов избежать атаки путем использования социальной инженерии являются следующие рекомендации:
• Проверять источник, не следует доверять всем, кто пишет вам в социальных сетях, даже своим близким, потому что их страницу могут взломать и под их именем просить перейти по ссылке или перевести деньги. Необходимо обязательно убедиться, что это именно твой близкий родственник или друг, например позвонить ему или задать дополнительные уточняющие вопросы, которые знает только он;
• Прежде чем переходить к действиям остановитесь и подумайте, а правда ли это ваш близкий человек пишет или нет. Так как в социальной инженерии используют срочность, чтобы жертва не смогла опомниться. Всего минута размышлений позволит вам выявить и предотвратить атаку;
• Используйте надежный спам-фильтр данная рекомендации поможет уменьшить количество мошеннических писем на вашу электронную почту.
1) Фишинг. Под фишингом понимается вид интернет-мошенничества путем использования поддельных сайтов или приложения, чтобы получить идентификационные данные пользователей. Как правило, фишинговая атака представляет собой выдачу фейковых сайтов, которые имитируют интрнет-страницы популярных компаний. Данный вид атаки пользует невнимательность пользователей. Для примера использования фишингового сайта сайт злоумышленника www.snils-m.online и официальный сайт налоговой службы www.nalog.ru.[5] Так все государственные сайты имеют множество страниц перехода, новостные ссылки своей деятельности, сайт защищен протоколом https используются специальные средства для людей с ограниченными возможностями, рисунок 6.

2. Разработка сайта по безопасности в социальных сетях

В ходе данной работы был разработан сайт для популяризации безопасного использования социальных сетей. Сайт состоит из нескольких элементов: Общая информация для чего нужен сайт, которая представлена на рисунке 11.

ЗАКЛЮЧЕНИ

В ходе выполнения данной работы были получены представления о безопасности в социальных сетях в области «Информационная безопасность», было углублено и расширенно теоретическое знание об основах информационной безопасности соцсетях, выявили основные опасности, классификацию угроз проанализировали информации по данной тематике на основе материалов научно-технических публикаций и Интернет-ресурсов.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Positive technologies, Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/;
2. Воронкин А.С., Социальные сети: эволюция, структура, анализ [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/sotsialnye-seti-evolyutsiya-struktura-analiz/viewer;
3. Sostav, Global Digital 2022: вышел ежегодный отчёт об интернете и социальных сетях — главные цифры [Электронный ресурс] – Режим доступа: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html;
4. Коршинов А.С., Защита личной информации в IT-сфере/2018. №16. – С. 35-39 [Электронный ресурс] – Режим доступа: http://www.danish-science.org/wp-content/uploads/2018/10/DSJ_16.pdf
5. Сайт Федеральной Налоговой Службы (ФНС России) [Электронный ресурс] – Режим доступа: https://www.nalog.gov.ru/rn77/
6. Федеральный закон «Об обязательном медицинском страховании в Российской Федерации» от 29.11.2010 N 326-ФЗ [Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_107289/