УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Макаров С.А., студент 3 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, социальные сети, безопасность, защита данных.*

Научная Статья посвящена анализу информационной безопасности социальных сетей. В то же время социальные сети, то есть информация в их рамках, становятся желаемым объектом мошеннических транзакций и незаконных действий по краже личных данных, которые могут использоваться для аутентификации на различных ресурсах и платформах.

Информационная безопасность в социальных сетях – это обеспечение защиты личной информации и данных пользователей, а также предотвращение угроз и рисков, связанных с использованием социальных сетей.

Современные социальные сети стали неотъемлемой частью повседневной жизни миллионов людей по всему миру. Однако, вместе с удобством и возможностью общения, они также представляют собой потенциальную угрозу для безопасности и конфиденциальности пользовательских данных. В последние годы проблемы информационной безопасности в социальных сетях стали все более актуальными, требуя комплексного подхода к их решению.

Информационная безопасность в социальных сетях становится все более важной из-за растущего количества пользователей и объема информации, которую они делятся в сети. Утечка персональных данных, кибербуллинг, фейковые новости, фишинг и другие угрозы могут негативно повлиять на пользователей и привести к серьезным последствиям.

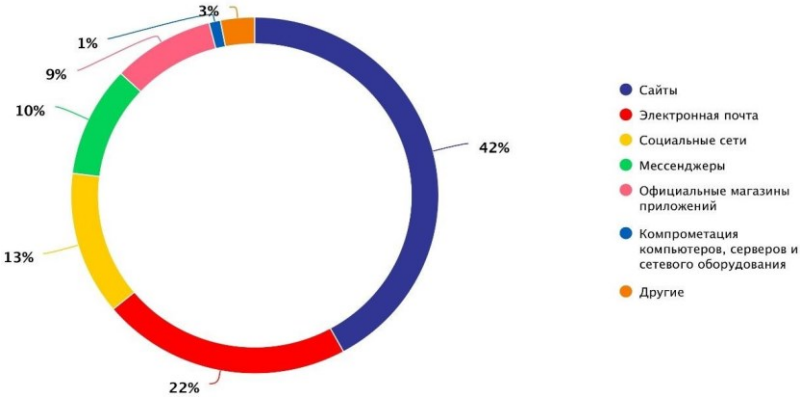

Рис. 1 – используемые злоумышленниками каналы социальной инженерии

Ключевым объектом информационной безопасности в социальных сетях выступает защита личных и персональных данных, которые выступают набором организационных, технических и организационно-технических мероприятий, направленных на защиту информации, что относится к конкретной личности [3].

Очевидно, что публикация персональных данных в социальных сетях, а также их изменение без согласия субъекта, приводит к негативным последствиям для последнего.

В рамках информационной безопасности, главной задачей является защита персональных данных от возможной ее кражи. В случае обратного процесса, в руках злоумышленников содержится инструмент, которые позволяет проводить анализ социальной структуры общества (в случае массовой кражи личных данных) и отдельной личности. Данные о пользователях социальных сетей могут быть проданы третьим лицам, так как соглашение с пользователями не запрещает этого. На сегодняшний день, социальные сети в Интернете являются весьма привлекательными сервисами, позволяющими получить коммерческую выгоду из анализа их данных [1].

Для борьбы с угрозами информационной безопасности в социальных сетях необходим комплексный подход. Это включает в себя использование современных технологий шифрования данных,

двухфакторной аутентификации, механизмов контроля доступа и систем мониторинга.

Кроме того, важно обучать пользователей правилам безопасного поведения в сети, чтобы они могли распознавать потенциальные угрозы и защищать свою информацию [5].

Регулярные аудиты безопасности, обновление программного обеспечения, использование антивирусов и защита от фишинга также являются важными шагами для обеспечения безопасности в социальных сетях. Конкретные меры по обеспечению информационной безопасности в социальных сетях могут включать следующие шаги:

1. Сильные пароли и двухфакторная аутентификация: рекомендуется использовать сложные пароли, состоящие из комбинации букв, цифр и символов. Двухфакторная аутентификация добавляет дополнительный уровень защиты, требуя подтверждение логина через другое устройство или метод, например, SMS-код.

2. Настройки конфиденциальности: необходимо проверьте и настроить настройки конфиденциальности в своем профиле, чтобы контролировать, кто может видеть вашу информацию и какие данные доступны для других пользователей.

3. Обучение пользователям: проведение обучающих мероприятий для пользователей о том, как распознавать потенциальные угрозы, как не становиться жертвой фишинга и как обращаться с личной информацией в сети.

4. Мониторинг активности: регулярно проверяйте свой аккаунт на подозрительную активность, необычные сообщения или запросы друзей. Если что- то кажется подозрительным, не стесняйтесь сообщить об этом администрации социальной сети.

5. Антивирусное программное обеспечение: установить и регулярно обновляйте антивирусное программное обеспечение на своем устройстве для защиты от вредоносных программ и кибератак [2].

Осторожность при кликах: быть осторожным при нажатии на ссылки в сообщениях или комментариях, особенно если они приходят от незнакомых пользователей. Это может быть попытка фишинга или вредоносного программного обеспечения.

1.Регулярные обновления: проверять, что ваше программное обеспечение и приложения всегда обновлены до последних версий, чтобы исправить уязвимости и обеспечить безопасность данных.

2. Безопасное общение: избегать обсуждения чувствительной информации, такой как пароли, номера кредитных карт или личные данные, в открытых чатах или комментариях.

3. Сообщайте о нарушениях: если вы столкнулись с кибербуллингом, нежелательными сообщениями или другими формами онлайн-нападений, не стесняйтесь сообщить об этом администрации социальной сети [3].

Ключевым объектом информационной безопасности в социальных сетях выступает защита личных и персональных данных, которые выступают набором организационных, технических и организационно-технических мероприятий, направленных на защиту информации, что относится к конкретной личности.

Очевидно, что публикация персональных данных в социальных сетях, а также их изменение без согласия субъекта, приводит к негативным последствиям для последнего [4].

В рамках информационной безопасности, главной задачей является защита персональных данных от возможной ее кражи. В случае обратного процесса, в руках злоумышленников содержится инструмент, которые позволяет проводить анализ социальной структуры общества (в случае массовой кражи личных данных) и отдельной личности. Данные о пользователях социальных сетей могут быть проданы третьим лицам, так как соглашение с пользователями не запрещает этого. На сегодняшний день, социальные сети в Интернете являются весьма привлекательными сервисами, позволяющими получить коммерческую выгоду из анализа их данных.

Библиографический список:

1. Белякова, Е. И. Угрозы информационной безопасности в социальных сетях: анализ и рекомендации по защите данных / Е.И. Белякова, Д.П. Григорьев // Журнал компьютерной безопасности и защиты информации. – 2022. - № 8. – С. 56-70.

2. Попов, С. Д. Информационная безопасность в социальных сетях: основные проблемы и пути их решения / С.Д. Попов, Н.М.

Степанова // Электронный журнал "Информационная безопасность". – 2021. – С. 33-47.

3. Шестакова Я. Безопасность персональных данных в социальных сетях / Я. Шестакова // Гуманитарные научные исследования. - 2020. - № 11. - С. 47-51.

4. Кривоухов А.А. Оценка информационной безопасности интернет- среды пользователями социальных сетей / А.А. Кривоухов // Коммуникология. - 2021. - №1. – С. 181-185

5. Голубев С.В. Актуальные вопросы информационной безопасности // / С.В. Голубев, С.А. Голбуева // Материалы научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». - Ульяновский ГАУ. – 2022. – С. 552-557.

INFORMATION SECURITY IN SOCIAL NETWORKS

Makarov S.A.
Scientific supervisor – Golubev S.V.
FSBEI HE Ulyanovsk SAU

Keywords: *information security, social networks, security, data protection.*

The scientific article is devoted to the analysis of information security of social networks. At the same time, social networks, i.e. the information within them, are becoming a desirable target for fraudulent transactions and illegal identity theft activities, which can be used for authentication on various re- sources and platforms.