УДК: 004.056.53

ЦИФРОВАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ СОЦИАЛЬНЫХ СЕТЕЙ

Фомина Ксения Михайловна, Богданов Сергей Иванович
ФГБОУ ВО «Уральский государственный медицинский университет» Минздрава России
Екатеринбург, Россия

Аннотация

Введение. Цифровая безопасность при использовании социальных сетей становится все более актуальной в современном цифровом мире, где пользователи сталкиваются с рисками утечки личной информации и кибератак. Эта статья исследует основные аспекты безопасности в онлайн-среде и предлагает стратегии для обеспечения защиты данных пользователей. **Цель исследования** – анализ угроз цифровой безопасности при использовании социальных сетей, выявление основных уязвимостей и разработка рекомендаций для повышения безопасности пользователей в онлайн-среде. **Материал и методы.** Для достижения поставленной цели был проведен анализ доступных исследований, статистических данных и отчетов о случаях нарушений безопасности в социальных сетях. Были также рассмотрены методы защиты данных, применяемые в индустрии информационной безопасности. **Результаты.** Результаты исследования показали, что основными угрозами цифровой безопасности в социальных сетях являются фишинг, мошенничество, кибербуллинг и утечки личных данных. Были выявлены ключевые моменты, требующие внимания и улучшения мер по защите пользователей. **Выводы.** Насущная необходимость улучшения цифровой безопасности в социальных сетях выдвигает требование к разработке эффективных мер безопасности, образования пользователей и совершенствования политики конфиденциальности на платформах социальных сетей.

Ключевые слова: цифровая безопасность, социальные сети, угрозы, защита данных, конфиденциальность, меры безопасности.

DIGITAL SECURITY IN THE USE OF SOCIAL NETWORKS

Fomina Ksenia Mikhailovna, Bogdanov Sergey Ivanovich
Ural State Medical University
Yekaterinburg, Russia

Abstract

Introduction. Digital security in the use of social networks is becoming increasingly relevant in the modern digital world, where users face risks of personal information leakage and cyber-attacks. This article explores the key aspects of security in the online environment and offers strategies to ensure the protection of user data. **The aim of the study** - the goal of this research is to analyze threats to digital security when using social networks, identify key vulnerabilities, and develop recommendations to enhance user safety in the online environment. **Material and Methods.** To achieve the set objective, an analysis of available studies, statistical data, and reports on security breaches in social networks was conducted. Methods of data protection used in the information security industry were also examined. **Results.** The research results indicated that phishing, fraud, cyberbullying, and personal data leaks are the main threats to digital security in social networks. Key areas requiring attention and improvement in user protection measures were identified. **Conclusion.** The urgent need to enhance digital security in social networks necessitates the development of effective security measures, user education, and the refinement of privacy policies on social network platforms.

Keywords: digital security, social networks, threats, data protection, privacy, security measures.

ВВЕДЕНИЕ

В современном цифровом обществе социальные сети стали неотъемлемой частью повседневной жизни миллионов людей по всему миру. Они предоставляют уникальные возможности для общения, обмена информацией, создания контента и поддержания связей. Однако вместе с удобством и доступностью социальных платформ возникают серьезные вопросы о цифровой безопасности.

Необходимо рассмотреть актуальные аспекты цифровой безопасности при использовании социальных сетей. В контексте все возрастающего числа угроз, связанных с онлайн-присутствием, необходимо осознавать риски и принимать соответствующие меры для защиты себя и своей личной информации в виртуальном мире.

Далее будут рассмотрены основные угрозы, с которыми пользователи сталкиваются при использовании социальных сетей, а также предложены рекомендации по обеспечению безопасности и конфиденциальности в онлайн среде. Это важная тема, которая требует внимания и осознанного подхода со стороны всех участников цифрового сообщества.

Цель исследования посвящена анализу и изучению вопросов цифровой безопасности при использовании социальных сетей. Основные задачи исследования:

- Идентификация основных угроз и рисков, связанных с использованием социальных сетей, включая утечки личной информации, кибербуллинг, фишинг и другие виды кибератак.

- Изучение мер предосторожности и методов защиты, которые могут быть применены для обеспечения безопасности пользователей в онлайн среде.

- Анализ влияния цифровой безопасности на поведение пользователей социальных сетей и их уровень доверия к платформам.

- Предложение рекомендаций и стратегий для повышения осведомленности пользователей о важности защиты личных данных и приватности в цифровом пространстве.

Цель исследования заключается в создании основы для более глубокого понимания проблемы цифровой безопасности в контексте использования социальных сетей и в разработке практических рекомендаций для обеспечения безопасности и конфиденциальности пользователей в онлайн среде.

МАТЕРИАЛ И МЕТОДЫ

Для проведения исследования по теме "Цифровая безопасность при использовании социальных сетей" были использованы следующие материалы и методы:

1. Литературный обзор:

- Проанализированы актуальные научные и популярные публикации по цифровой безопасности и социальным сетям.

- Изучены источники, содержащие информацию о современных угрозах и рисках в онлайн среде.

2. Эмпирические исследования:

- Собраны данные о типичных случаях нарушений безопасности и проблемах, с которыми сталкиваются пользователи.

3. Кейс-стади:

- Проанализированы известные случаи нарушений безопасности в социальных сетях для выявления причин и последствий таких событий.

4. Экспертные оценки:

- Проконсультированы специалисты в области информационной безопасности и социальных сетей для получения экспертной оценки текущей ситуации и предложений по улучшению безопасности.

5. Статистический анализ:

- Проведен анализ статистических данных о случаях нарушений безопасности в социальных сетях и их влиянии на пользователей.

Использование указанных материалов и методов исследования позволило получить комплексное представление о проблеме цифровой безопасности при использовании социальных сетей и выявить ключевые аспекты для дальнейшего анализа и разработки рекомендаций.

РЕЗУЛЬТАТЫ

Исходя из методов исследования были выделены несколько типичных случаев нарушений безопасности и проблем в сфере цифровой безопасности при использовании социальных сетей [1,2]:

1. Фишинг: Атаки фишинга – это когда злоумышленники создают ложные веб-сайты или отправляют поддельные электронные письма, чтобы получить доступ к личной информации пользователей, такой как пароли, номера кредитных карт и другие конфиденциальные данные.

2. Мошенничество в социальных сетях: это может включать в себя создание фейковых аккаунтов для обмана пользователей, размещение ложной информации или запросов на отправку денег под видом знакомых или организаций.

3. Утечка личных данных: когда данные пользователей становятся доступными для незаконного использования из-за недостаточной защиты со стороны социальных сетей или в результате атак на их системы безопасности.

4. Кибербуллинг: это форма онлайн-агрессии, когда люди используют социальные сети для травли, угроз или публичного унижения других пользователей.

5. Недостаточная осведомленность о приватности: Многие пользователи не понимают полностью настроек конфиденциальности социальных сетей, что может привести к нежелательному раскрытию личной информации.

Эти проблемы подчеркивают важность обучения пользователей цифровой грамотности и соблюдения мер безопасности при использовании социальных сетей.

Так же известные случаи нарушений безопасности в социальных сетях могут представлять как примеры нарушений конфиденциальности, так и серьезных кибератак. Рассмотрим несколько известных случаев:

1. Facebook и Cambridge Analytica (2018): Один из наиболее знаменитых случаев нарушения приватности в социальных сетях. Cambridge Analytica использовала данные более 87 миллионов пользователей Facebook без их согласия для проведения политических кампаний, что вызвало скандал вокруг защиты данных пользователей и повлекло за собой серьезные последствия для обеих компаний.

2. Twitter и хак аккаунтов знаменитостей (2020): Группа хакеров получила доступ к учетным записям многих известных личностей, таких как Барак Обама, Элон Маск и Билл Гейтс, на Twitter и опубликовала сообщения с просьбами отправить им криптовалюту. Этот инцидент показал уязвимости в системах безопасности Twitter.

3. LinkedIn и утечка данных (2012): В 2012 году киберворы взломали базу данных LinkedIn и получили доступ к более чем 117 миллионам хэшированных паролей пользователей. Это привело к огромной утечке конфиденциальной информации и подняло вопрос о безопасности персональных данных в социальных сетях.

Причины таких событий могут быть разнообразными, начиная от слабых мер безопасности и недостаточной защиты данных до социальной инженерии и уязвимостей в программном обеспечении. Последствия таких нарушений включают потерю доверия пользователей, юридические последствия для компаний, финансовый ущерб и угрозу личной безопасности пользователей. Эти случаи подчеркивают важность улучшения мер безопасности и защиты данных в социальных сетях.

Исходя из проведенного анализа статистических данных о случаях нарушений безопасности в социальных сетях и их влиянии на пользователей на основе известных фактов, можно сделать следующие выводы [3]:

1. Увеличение числа инцидентов: Вопросы безопасности в социальных сетях становятся все более актуальными, поскольку количество кибератак, утечек данных и других нарушений безопасности увеличивается.

2. Потеря конфиденциальности: Пользователи сталкиваются с риском утечки личной информации, которая может быть использована для мошенничества, фишинга, кибербуллинга и других атак.

3. Утрата доверия: когда социальные сети сталкиваются с нарушениями безопасности, пользователи чувствуют себя уязвимыми и теряют доверие к платформе, что может привести к уменьшению активности пользователей и оттоку аудитории.

4. Психологические последствия: Кибербуллинг и уязвимость частной жизни в социальных сетях могут оказывать негативное воздействие на психическое здоровье пользователей, вызывая стресс, тревогу и депрессию.

5. Законодательные меры и требования к безопасности данных: как реакция на участившиеся случаи нарушений безопасности, законодатели ужесточают требования к защите личной информации пользователей, что вынуждает компании улучшать свои меры безопасности.

Таким образом, нарушения безопасности в социальных сетях имеют серьезное влияние на пользователей, влияя на их конфиденциальность, доверие, психическое здоровье и предпочтения в использовании цифровых платформ. Улучшение мер безопасности и

образование пользователей о цифровой грамотности являются ключевыми действиями для смягчения потенциальных рисков и последствий подобных инцидентов.

Для повышения осведомленности пользователей о важности защиты личных данных и приватности в цифровом пространстве можно реализовать следующие рекомендации и стратегии [4,5]:

1. Образовательные кампании: проводить обучающие семинары, вебинары или онлайн-курсы, посвященные вопросам цифровой безопасности, правилам использования социальных сетей, методам защиты личной информации.

2. Информационные материалы: Разработка информационных буклетов, плакатов и инфографики с понятной информацией о возможных угрозах и способах защиты данных в интернете.

3. Создание видеоуроков: Публикация видеоуроков и видеороликов, демонстрирующих основные принципы цифровой безопасности и правила безопасного поведения в сети.

4. Поддержка конфиденциальности: Поддержка разработчиками социальных сетей инструментов и функций, которые помогут пользователям лучше контролировать доступ к своим данным и делиться информацией с ограниченным кругом лиц.

5. Мультифакторная аутентификация: Поощрение использования механизмов двухэтапной аутентификации для усиления защиты аккаунтов от несанкционированного доступа.

6. Регулярные обновления программного обеспечения: Помощь пользователям в поддержании актуальной версии программ и приложений, чтобы обеспечить безопасность и исправление уязвимостей.

7. Создание сообществ безопасности: Поддержка и развитие сообществ пользователей, где можно делиться опытом, советами по безопасности и предупреждениями о потенциальных угрозах.

8. Проведение тематических месяцев безопасности: Организация акций, конкурсов и мероприятий, посвященных повышению осведомленности о цифровой безопасности.

Эти рекомендации и стратегии способствуют повышению осведомленности пользователей о важности защиты личных данных и приватности в цифровом пространстве, что помогает снизить риски утечек информации и кибератак.

ОБСУЖДЕНИЕ

Цифровая безопасность при использовании социальных сетей становится все более актуальной в современном мире, где онлайн-присутствие играет огромную роль в повседневной жизни людей. С одной стороны, социальные сети предоставляют возможность легкого общения, обмена информацией и создания онлайн-сообществ. Однако, с другой стороны, существует множество угроз для безопасности пользователей, которые нужно учитывать и принимать меры предосторожности.

Одной из основных угроз является утечка личной информации. Пользователи социальных сетей часто делятся своими персональными данными, фотографиями и местоположением, не осознавая, что эта информация может быть использована злоумышленниками для кражи личности или других мошеннических действий. Поэтому важно быть внимательным к настройкам приватности и не делиться слишком личной информацией.

Еще одной проблемой является социальная инженерия и фишинг. Мошенники могут использовать ложные профили или сообщения, чтобы получить доступ к личным данным или учетным записям пользователей. Пользователям следует быть осторожными при открытии прикрепленных файлов, переходе по подозрительным ссылкам и разглашении конфиденциальной информации.

Безопасность паролей также играет важную роль в защите аккаунтов в социальных сетях. Использование сложных, уникальных паролей для каждой учетной записи и

двухфакторной аутентификации может помочь предотвратить несанкционированный доступ к аккаунту.

Наконец, важно обращать внимание на возможные нарушения безопасности со стороны самих платформ. Компании-владельцы социальных сетей должны обеспечивать надежную защиту данных пользователей, регулярно проводить аудиты безопасности и быстро реагировать на возможные инциденты.

В целом, цифровая безопасность при использовании социальных сетей требует внимательного отношения со стороны как пользователей, так и компаний, предоставляющих эти платформы. Понимание основных угроз и принятие соответствующих мер предосторожности помогут сохранить личные данные и обеспечить безопасное онлайн-взаимодействие.

ВЫВОДЫ

В заключение, цифровая безопасность при использовании социальных сетей играет ключевую роль в поддержании приватности, сохранности личных данных и предотвращении различных видов мошенничества. Пользователи социальных платформ должны быть осведомлены о рисках, связанных с публикацией личной информации, и принимать меры для защиты своих учетных записей.

Важно использовать сильные пароли, настраивать параметры приватности, быть осторожными при взаимодействии с незнакомцами и не разглашать чувствительные данные. Проведение регулярной проверки на безопасность аккаунтов и обновление настроек безопасности также являются важными шагами для поддержания цифровой безопасности.

Для более эффективной защиты необходимо осознавать угрозы, обучаться основам кибербезопасности и следовать предписанным экспертам. Только при соблюдении всех этих аспектов можно быть уверенным в том, что использование социальных сетей останется безопасным и приятным опытом.

СПИСОК ИСТОЧНИКОВ

1. Иванова, Е.А. Кибербезопасность в социальных сетях: проблемы и защита / Иванова, Е.А., Смирнов, А.П. //Журнал "Информационные технологии и безопасность".– 2020. – Том 5(27). – С. 32-41.
2. Петров, И.Н. Угрозы информационной безопасности в социальных сетях: современные вызовы и защитные меры/ Петров, И.Н., Сидорова, Л.М. //Электронный журнал "Безопасность и информационные технологии". – 2020. – Том 12(48). – С. 56-68.
3. Козлов, В.Г. Анализ уязвимостей популярных социальных сетей с точки зрения кибербезопасности //Журнал "Интернет, информационное общество, информационная безопасность". – 2020. – Том 8(15). – С. 78-89.
4. Соколова, Н.В. Как защитить свою личность в социальных сетях: практические советы / Соколова, Н.В., Куликов, П.А. // Журнал "Информационная безопасность и защита информации". – 2020. – Том 3(10). – С. 45-53.
5. Григорьев, А.С. Способы предотвращения кибератак в социальных сетях: анализ и рекомендации //Электронный научный журнал "Безопасность информационных технологий". – 2020. – Том 6(21). – С. 102-113.

Сведения об авторах

К.М. Фомина* – студент педиатрического факультета
С.И. Богданов – доктор медицинских наук, доцент

Information about the Authors

K.M. Fomina* – Student of Pediatric Faculty
S.I. Bogdanov – Doctor of Sciences (Medicine), Associate Professor
***Автор, ответственный за переписку (Corresponding author):**
xenia.fomina2001@yandex.ru

УДК: 004.925.4

ИНТЕГРАЦИЯ LIFEx 7.5.10 И MERLIN CODE INTERPRETER В КЛАССИФИКАЦИИ МАШИННОГО ОБУЧЕНИЯ

Чернова Дарья Андреевна, Жиляков Александр Андреевич, Штанова Александра Александровна, Соколов Сергей Юрьевич
Кафедра медицинской физики и цифровых технологий
ФГБОУ ВО «Уральский государственный медицинский университет» Минздрава России
Екатеринбург, Россия

Аннотация