СТРАТЕГИИ АТАК В СЕТИ ИНТЕРНЕТ И СПОСОБЫ ЗАЩИТЫ

А.В. Машков, *канд. техн. наук, доцент*
А.А. Галеев, *студент*
Самарский государственный технический университет
(Россия, г. Самара)

DOI:10.24412/2500-1000-2026-2-1-231-236

Аннотация. *Активное использование социальных сетей и мессенджеров перетекает в риски, связанные с несанкционированным доступом к учетным записям пользователей. В связи с этим обеспечение конфиденциальности личной информации становится критически важной задачей. В данной статье рассматриваются и анализируются ключевые угрозы информационной безопасности на современных платформах в просторах сети Интернет и предлагается комплекс практических мер, направленных на минимизацию уязвимости персональных данных.*

Ключевые слова: *приватность; персональные данные; социальные сети; аутентификация; биометрическая защита; фишинг.*

Современные социальные сети – это не просто инструменты общения, но и масштабные хранилища персональных данных: от базовых анкетных сведений до различных поведенческих действий. Активное взаимодействие в социальных сетях создает непропорциональную ситуацию: стремление к открытому общению конфликтует с необходимостью сохранения приватности персональных данных. Хакеры в сети Интернет применяют большое количество способов с целью взлома личных конфиденциальных данных различных аккаунтов пользователей: проводят изменение внешнего вида профиля и всех его составляющих, отправляют сообщения с просьбой подтвердить учетные записи, присылают предложения, которые затрагивают и привлекают людей выполнять действия, указанные в них, ненастоящие предупреждения о подозрительной активности, создают фальшивые вебсайты, которые очень похожие на официальные сайты компаний.

Проблема, которая представляет собой утечку сведений, даже кажущихся незначительными в результате анализа больших данных, может привести к серьезным последствиям, включая мошенничество, шантаж или ущерб со стороны человеческой позиции. Утечки могут происходить как в результате атак злоумышленников, так и из-за невнимательного и необдуманного поведения пользователей.

Одним из распространенных векторов атак является целевой фишинг. В отличие от массовых рассылок, подобные атаки характеризуются высокой степенью персонализации. Злоумышленники проводят детальный анализ профиля жертвы в социальных сетях, определяя круг общения, интересы и индивидуальный стиль коммуникации. Сформированные на этой основе сообщения могут имитировать взаимодействие от реальных друзей, коллег или сервисов, которыми пользуется жертва [1]. Типичным примером служит письмо, маскирующееся под уведомление от службы поддержки социальной сети о подозрительной активности и содержащее ссылку на фальшивую страницу входа. Так, The Daily Swig сообщила о фишинговой атаке, произошедшей в декабре 2020 года на американского поставщика медицинских услуг Elara Caring, которая произошла после несанкционированного компьютерного вторжения, нацеленного на двух его сотрудников. Злоумышленник получил доступ к электронной почте сотрудников, в результате чего были раскрыты личные данные более 100 000 пожилых пациентов [2].

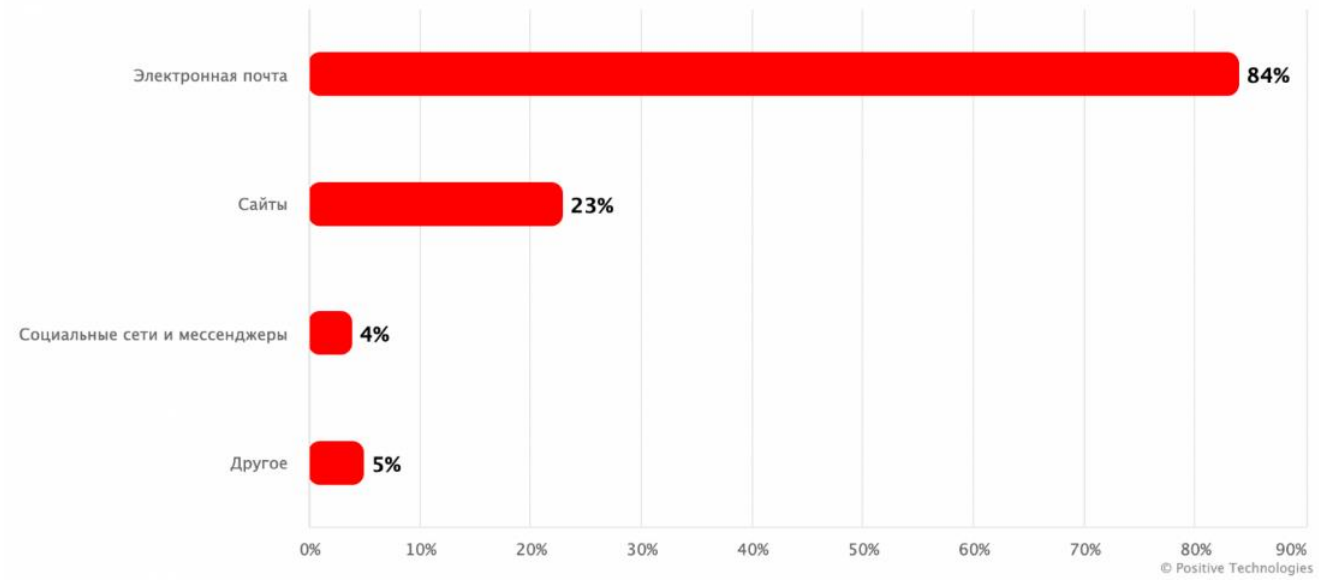

Рис. 1. Основные каналы, используемые злоумышленниками для фишинговой атаки за 2024 год

Отдельное место занимает квишинг – использование QR-кодов в новых атаках. Пользователю предлагается отсканировать код для получения «эксклюзивного доступа», «подарка» или «проверки безопасности аккаунта». Данный QR-код осуществляет перенаправление на фишинговый веб-сайт, который при просмотре с мобильного устройства выглядит особенно убедительно [3].

Высокой эффективностью отличаются атаки, эксплуатирующие доверие через взломанные аккаунты. В рамках данной техники злоумышленник получает доступ к профилю друга или родственника жертвы. От имени этого доверенного лица отправляются сообщения с просьбой о помощи, например, о срочной необходимости некоторого количества денежных средств в связи с кражей телефона или какими-либо случившимися серьезными обстоятельствами, где часто могут содержаться подозрительные и вредоносные ссылки.

Также серьезной угрозой безопасности онлайн-пользователей является вредоносное ПО. Злоумышленники распространяют вирусы, маскируя их под привлекательные ссылки и приложения. Нажав на такие ссылки, пользователи рискуют заразить свои устройства, что может привести к утечке личной информации или шифрованию данных с требованием выкупа. Исследования показывают, что среднестатистический пользователь имеет от 5 до 10 аккаунтов в различных социальных сетях, каждый из которых содержит уникальные комбинации данных: от явной информации (имя, возраст, фотографии) до скрытых поведенческих паттернов (время активности, скорость прокрутки, эмоциональная реакция на контент).

Например, троянцы семейства «Stealer», предназначено для кражи файлов cookies сессий, паролей, сохраненных в браузере, и токенов доступа. Попадая на устройство, такие программы позволяют злоумышленнику получить доступ к аккаунтам жертвы, минуя двухфакторную аутентификацию, даже без знания паролей [4].

Распространенным вектором являются атаки на инфраструктуру OAuth. Многие приложения используют данный протокол для авторизации через социальные сети. Мошенники создают фальшивые приложения, которые запрашивают чрезмерные права доступа, такие как «Управление вашим аккаунтом». Предоставление согласия пользователем в такой ситуации фактически означает передачу полного контроля над профилем злоумышленнику.

К скрытым угрозам относится криптоджекинг через социальные сети. Вредоносные скрипты, встраиваемые в рекламные объявления или посты, тайно используют вычислительные мощности устройства жертвы для майнинга криптовалюты. Это приводит к перегреву и ускоренному износу оборудования без ведома пользователя. Основные риски для пользователей включают утечку контактных данных, раскрытие и возможность отслежи-

вания геолокационной информации, кражу цифровых идентификаторов, а также различные формы манипуляций с персональными сведениями. Рассматривая произошедший случай данной опасности, в 2019 году из Microsoft Store было удалено восемь отдельных приложений, которые тайно добывали криптовалюту за счет ресурсов загрузивших их пользователей. При загрузке и запуске приложений происходила загрузка кода JavaScript для криптоджекинга. После чего на устройстве активировался майнер и начинался поиск криптовалюты Monero с использованием значительной части ресурсов устройства, что замедляло его работу [5].

Смоделирую вышеперечисленную совокупность видов кибератак в понятную и наглядную схему (рис. 2).

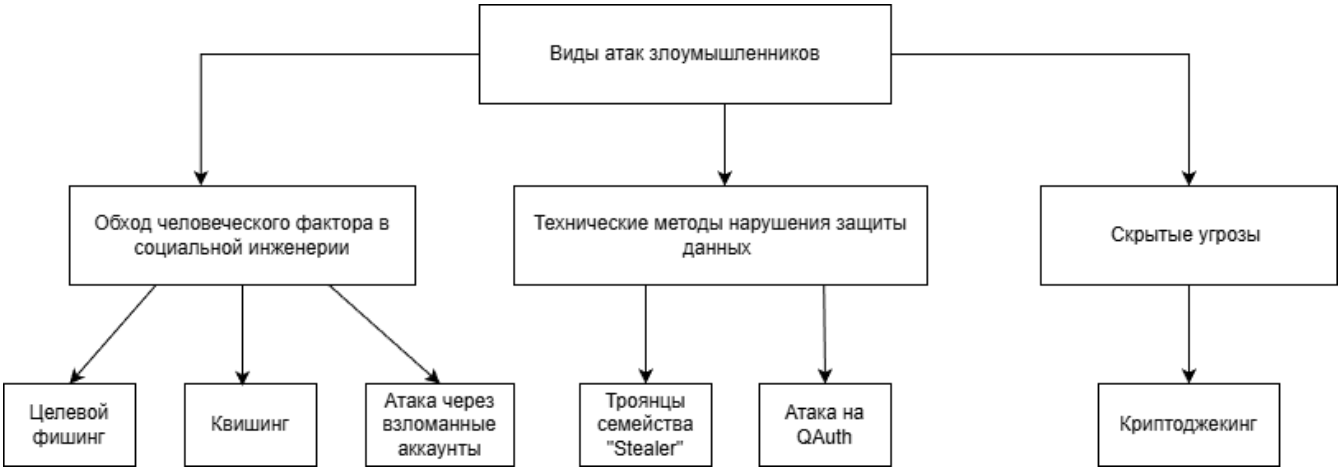

Рис. 2. Схематичное представление видов информационно-технических атак в сети Интернет

Причинами всему вышеперечисленному часто становятся следующие факторы:

- использование ненадежных паролей;
- публикация избыточной личной информации;
- невнимательность при переходе по каким-либо ссылкам.

Критическими последствиями взлома аккаунта становятся:

- геолокация данных в реальном времени;
- определение сетевого окружения устройства через параметры точек беспроводного доступа;
- получение полного доступа к телефонной книге и истории коммуникаций, привязанных к номеру телефона. Эти данные становятся основой для последующих атак, включая социальную инженерию, шантаж и финансовое мошенничество.

Отдельного внимания заслуживает растущая угроза кросс-платформенной компрометации. Злоумышленники все чаще используют технику OSINT (разведка на основе открытых источников), собирая информацию о жертве из разных утечек (сервисы доставки, форумы, устаревшие профили) и компилируя их в единый ключ для взлома основного аккаунта. Например, номер телефона из старой базы данных, дата рождения из открытого профиля могут стать исчерпывающим набором для восстановления пароля или ответа на контрольный вопрос.

Для минимизации рисков требуется последовательное соблюдение базовых правил безопасности и применение ряда специализированных инструментов защиты [6].

Использование надежных паролей. Во избежание нарушения безопасности со стороны злоумышленников в социальных сетях и на всех онлайн-площадках следует использовать надежный пароль, который будет содержать в себе такие параметры, как: минимальная длина пароля от 8 символов, комбинация заглавных/строчных букв, цифр и спецсимволов, отсутствие логичных и понятных подсказок, подразумевающих под собой даты рождения, имена близких, а также использование уникальных паролей для каждого социального сервиса. Кроме того, необходимо часто проводить смены паролей на новый набор букв, символов и цифр – для критически важных сервисов рекомендуется обновлять их не реже, чем раз в квартал. Но недостаточно только составить сложный пароль, нужно его

еще где-то хранить, тем самым, один из методов – использование длинных фраз или предложений, которые легко запоминаются. Разделение пароля на части и регулярная практика его ввода способствуют лучшему запоминанию.

Двухфакторная аутентификация (2FA). Существенным барьером для злоумышленников является двухфакторная аутентификация. Данный метод требует от пользователей представления двух форм аутентификации для доступа к учетной записи – сочетание чего-то, что пользователь знает (например, пароль), и чего-то, что у него есть (например, код, отправленный на мобильный телефон). Есть несколько видов реализации 2FA:

- пароль + SMS/звонок;
- пароль + приложение-аутентификатор (например, Google Authenticator) или пароль + push-уведомление (Google, многие банковские системы);
- пароль + биометрия. Отпечаток пальца или Face ID [7].

Принцип минимальной достаточности данных. Следует сознательно ограничивать объем публикуемой личной информации, особенно касающийся распорядка дня, планов на отпуск и текущего местоположения. Эти сведения используются для социального инжиниринга и физической криминальной активности. Необходимо проводить регулярный «аудит приватности»: проверять, какая информация видна друзьям, подписчикам и всем пользователям сети, используя встроенные инструменты проверки просмотра профиля. Особенно важно контролировать метаданные, автоматически прикрепляемые к фотографиям.

Селективность в установлении контактов. Добавление в друзья незнакомых пользователей требует анализа их профиля на предмет признаков «фейковости». Диалоги с подозрительными собеседниками, запрашивающими личные данные или предлагающими перейти по сомнительным ссылкам, должны немедленно прекращаться.

В последние годы качественно новым фактором риска стало внедрение технологий искусственного интеллекта в практику киберпреступности. Генеративные нейросети позволяют создавать сверхреалистичный фальшивый контент – так называемые «дипфейки». Злоумышленники используют их для целевых атак на конкретных пользователей, например: с помощью голосовых клонов, а именно нескольких минут аудиозаписи из открытых источников создается модель голоса жертвы. Мошенники затем используют этот клон в телефонных звонках родственникам или коллегам, имитируя экстренную ситуацию и запрашивая денежный перевод; создание фальшивых видеообращений (видеоподделки), где публичная фигура или даже знакомый человек просит предоставить доступ к системам или перевести средства. Такие атаки обладают высокой убедительностью. ИИ может автоматически создавать правдоподобные изображения несуществующих людей и наполнять их профили контентом, что усложняет обнаружение ботов и мошеннических аккаунтов, это представляет собой генерацию фейковых (ненастоящих) профилей [8].

Успех большинства атак основан не на техническом превосходстве, а на эксплуатации психологии пользователя. Здесь рассматриваются следующие психологические аспекты:

- эффект срочности и авторитета – фишинговые сообщения часто создают искусственный дефицит времени или имитируют приказы от руководства, чтобы отключить критическое мышление жертвы;
- когнитивная перегрузка – сложные и намеренно запутанные интерфейсы настроек приватности приводят к «усталости от согласия». Пользователи механически принимают условия, не вчитываясь, лишь бы быстрее получить доступ к функционалу;
- социальное доказательство и доверие – мошенники создают целые сети взаимосвязанных фейковых профилей, которые «дружат» между собой и оставляют позитивные комментарии. Это формирует у жертвы ложное ощущение надежности и популярности злоумышленника.

На рисунке 2 изображена схема, которая показывает популярность угроз безопасности учетных записей в социальных сетях и различных платформах в просторах Всемирной паутины.

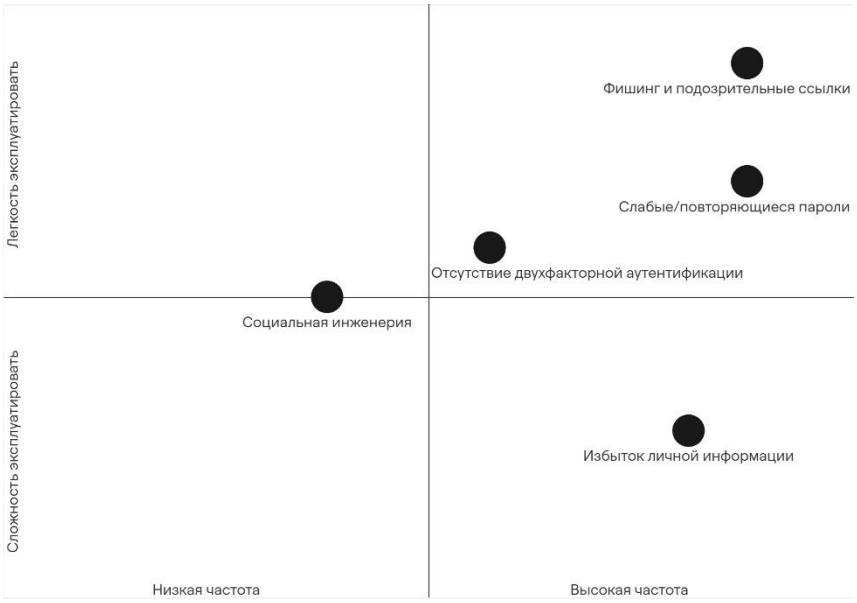

Рис. 2. Матрица опасности угроз для пользователей

На матрице приведены элементы (оси), которые обозначают следующие параметры:

- ось X – частота (частота встречи угрозы и их затрагивания пользователей);
- ось Y – простота эксплуатации для злоумышленника (легкость данного опасно риска использовать в атаке).

Тем самым, визуализируя соотношение двух этих осей по их соответствующим параметрам, можно сделать вывод, что: верхний правый ряд, где наблюдается легкость эксплуатации и высокая частота – самые опасные и приоритетные риски, которые требуют немедленных действий; верхний левый – незначительно опасные угрозы, часто решающиеся техническом путем, автоматизацией; нижний правый ряд представляет собой те риски, что редки, но катастрофичны, требующие ряда запланированных действий на случай чрезвычайной ситуации; нижний левый ряд – опасности с низким приоритетом, за которыми требуется лишь наблюдение.

Таким образом, в ходе проведенного исследования различных мошеннических атак в социальной ИТ-индустрии выяснилось, что современные платформы, став неотъемлемой частью жизни, создали парадоксальную ситуацию: стремление к открытому общению и самовыражению вступает в противоречие с фундаментальной потребностью безопасности. И, как показывает актуальность данной проблемы, мошенники сегодня атакуют именно не через какую-либо хакерскую техническую программу, а сквозь когнитивные искажения пользователей: доверие, любопытство, чувство срочности, минуя вдумчивость и внимательность людей.

Библиографический список

1. Фишинг. – [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3.
2. 11 типов фишинга и их примеры из реальной жизни. – [Электронный ресурс]. – Режим доступа: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/?ysclid=ml9qxvu32u26768953.
3. Морозова Е.В., Тюрпеко Е.С. Квишинг и современные реалии. – Кемерово, 2025.
4. Кристофер Х. Социальная инженерия в мошеннических схемах. – Москва, 2020.
5. Что такое криптоджекинг – определение и описание. – [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptojacking.
6. Дворянкин О.А. OSINT, PENTEST и НЕТСТАЛКИНГ – информационные технологии интернета. – Москва, 2022.
7. Сергеев В.Д. Метод двухфакторной аутентификации в облачном сервисе. – Санкт-Петербург, 2019.
8. Гигиена в социальных сетях. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/ussc/articles/884186/?ysclid=mlc0afzj1x223543415.

INTERNET ATTACK STRATEGIES AND PROTECTION METHODS

A.V. Mashkov, *Candidate of Technical Sciences, Associate Professor*
A.A. Galeev, *Student*
Samara State Technical University
(Russia, Samara)

Abstract. *The active use of social networks and messengers leads to risks associated with unauthorized access to user accounts. Therefore, ensuring the confidentiality of personal information has become a critical task. This article examines and analyzes the key threats to information security on modern platforms in the vastness of the Internet and proposes a set of practical measures aimed at minimizing the vulnerability of personal data.*

Keywords: *privacy; personal data; social networks; authentication; biometric protection; phishing.*