Научная статья
УДК 004.056.55:316.472.4
ББК 16.84:16.263.2
М 26
DOI: 10.53598/2410-3225-2024-2-341-51-61

Метод претекстинга как угроза информационной безопасности в социальных сетях

(*Рецензирована*)

Валерий Константинович Маркелов[1], Александр Николаевич Привалов[2]

[1] *Шуйский филиал Ивановского государственного университета*, *Шуя*, *Россия*, *v.a.l.e.m.a.r.k@yandex.ru*
[2] *Шуйский филиал Ивановского государственного университета*, *Шуя*; *Тульский государственный педагогический университет имени Л. Н. Толстого*, *Тула*, *Россия*, *privalov.61@mail.ru*

Аннотация. *В работе рассматривается феномен популярности социальных сетей, который обращает на себя внимание киберпреступников, которые считают социальные сети привлекательной средой для использования методов социальной инженерии с целью выманивания денежных средств и персональных данных пользователей социальных сетей. На основе проведенного количественного и качественного анализа публикаций в базах научных публикаций eLibrary и Google Scholar определены актуальные направления исследований по проблемам информационной безопасности в социальных сетях, одной из которых является проблема защищенности пользователей от атак социальной инженерии в социальных сетях, в том числе фишинга и претекстинга. Проведенный анализ публикаций в базах научных публикаций eLibrary, Scopus, Google Scholar за последние 10 лет по проблемам противодействия методам социальной инженерии в социальных сетях демонстрирует возрастающий интерес ученых к данной области исследований. Вместе с этим в последние годы наблюдается рост числа исследований, посвященных изучению претекстинга как метода социальной инженерии, однако количество исследований, посвященных проблеме претекстинга в социальных сетях, остается недостаточным. В заключение статьи предлагаются меры противодействия атакам социальной инженерии в социальных сетях с использованием претекстинга.*

Ключевые слова: *социальные сети, социальная инженерия, претекстинг, фишинг, защита информации, пользователи социальных сетей, информационная безопасность*

Для цитирования: *Маркелов В. К., Привалов А. Н. Метод претекстинга как угроза информационной безопасности в социальных сетях // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2024. Вып. 2 (341). С. 51–61. DOI: 10.53598/2410-3225-2024-2-341-51-61*

Original Research Paper

Pretexting method as a threat to information security in social networks

Valery K. Markelov[1], Aleksandr N. Privalov[2]

[1] *Shuya Branch of Ivanovo State University*, *Shuya*, *Russia*, *v.a.l.e.m.a.r.k@yandex.ru*
[2] *Shuya Branch of Ivanovo State University*, *Shuya*; *Tula State Pedagogical University named after L. N. Tolstoy*, *Tula*, *Russia*, *privalov.61@mail.ru*

Abstract. *The article examines the phenomenon of the popularity of social networks, which attracts the attention of cybercriminals who consider social networks an attractive environment for using social engineering methods in order to lure money and personal data from users of social networks. Based on the quantitative and qualitative analysis of publications in the databases of scientific publications eLibrary and Google Scholar, current areas of research on problems of information security in social networks, one of which is the problem of protecting users from social engineering at-*

tacks in social networks, including phishing and pretexting, are identified. An analysis of publications in the databases of scientific publications eLibrary, Scopus, Google Scholar over the past 10 years on the problems of countering social engineering methods in social networks demonstrates the growing interest of scientists in this area of research. At the same time, in recent years there has been an increase in the number of studies devoted to the study of pretexting as a method of social engineering, but the number of studies devoted to the problem of pretexting in social networks remains insufficient. In conclusion, the article proposes countermeasures for social engineering in social networks using pretexting.

Keywords: *social networks, social engineering, pretexting, phishing, information protection, social network users, information security*

For citation: *Markelov V. K., Privalov A. N. Pretexting method as a threat to information security in social networks // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2024. Iss. 2 (341). P. 51–61. DOI: 10.53598/2410-3225-2024-2-341-51-61*

В современном обществе социальные сети являются одним из основных инструментов для общения между пользователями в сети Интернет. Понятие «социальная сеть» было введено в 1954 году норвежским социологом Джеймсом Барнсом и прежде всего обозначает «социальную структуру, состоящую из множества субъектов (индивидов, социальных групп, организаций) и связей между ними, возникающими по поводу обмена ресурсами» [1]. В современном понимании, социальная сеть – это «онлайн-платформа, предназначенная для общения, поиска единомышленников и объединения людей в группы по интересам» [2].

Таким образом, социальная сеть – это «платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений, визуализацией которых являются социальные графы (графы, узлы которого представлены социальными объектами, такими как пользовательские профили с различными атрибутами (например: имя, день рождения, родной город и т. д.), сообщества, медиа-контент и т. д., а ребра – социальными связями между ними)» [3].

При этом социальные сети, как онлайн-сервисы для общения, реализуют следующие функции:

– коммуникативная (предоставляют возможности для коммуникации и поддержания связи между пользователями сети Интернет);

– развлекательная (предоставляют своим пользователям доступ к разнообразным формам развлекательного контента: фотографии, музыка, видео, сообщества, онлайн-игры и т.д., при этом пользователи могут просматривать фотографии и видео других пользователей социальной сети, слушать музыку, играть в онлайн-игры, принимать участие в развлекательных сообществах и т. п.);

– информационная (дают возможность обмениваться информацией с другими пользователями, причем такая информация «может относиться к элементам персонального характера (например, личные достижения и успехи, фотографии, личные данные), так и к элементам познавательного, новостного и обучающего характера» [4]);

– коммерческая (предоставляют своим пользователям площадку для продвижения бизнеса, а также рекламы товаров и услуг, в частности, основными целями присутствия бизнеса в социальных сетях являются: «привлечение дополнительного трафика (лидогенерация), например, на сайт компании для повышения объемов продаж; повышение лояльности клиентов компании благодаря «теплому», иногда неформальному взаимодействию; рост узнаваемости бренда; создание и/или улучшение имиджа компании; формирование репутации компании, бренда или продукта» [5]).

Причиной появления феномена социальных сетей является повышенная потребность в общении, которая свойственна людям, причем в настоящее время их популярность стремительно растет. Согласно отчету Digital 2024: Global Overview Report, по состоянию на январь 2024 года «число активных пользователей социальных сетей

насчитывает 5,04 миллиардов человек, что составляет 62,3 % населения планеты (январь 2023 года – 4,76 % миллиардов человек, 60 % населения планеты)» [6]. Данные отчета статистического портала Statista о самых популярных сетях в мире по состоянию на январь 2024 года показывают, что самые популярные социальные сети посещают более 3 млрд. активных пользователей в месяц [7]. Самыми популярными социальными сетями в России, согласно отчету аналитической компании MediaScope [8], являются ВКонтакте (месячный охват: 90 млн. пользователей в месяц, 74,0 % от населения страны) и Telegram (месячный охват: 84 млн. пользователей в месяц, 69,1 % от населения страны).

Феномен популярности социальных сетей не только привлекает миллионы пользователей по всему миру, но и обращает на себя внимание киберпреступников, которые считают социальные сети привлекательной средой для использования методов социальной инженерии с целью выманивания денежных средств и персональных данных пользователей социальных сетей.

При этом отметим, что в соответствии с Доктриной информационной безопасности Российской Федерации, одной из основных информационных угроз является «возрастание масштабов компьютерной преступности, а также увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе при обработке персональных данных с использованием информационных технологий, при этом методы, способы и средства совершения таких преступлений становятся все изощреннее» [9].

Являясь открытым источником информации, социальные сети могут использоваться киберпреступниками для проведения атак с использованием различных методов социальной инженерии, в том числе метода претекстинга. Термин «социальная инженерия» популяризирован в сфере информационной безопасности в начале XXI века известным хакером и специалистом по информационной безопасности Кевином Митником, согласно его определению, «социальная инженерия – это совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека» [10]. Кристофер Хаднеги, один из ведущих специалистов в области социальной инженерии, под социальной инженерией понимает «любые действия, подталкивающие другого человека сделать то, что может как пойти ему на пользу, так и навредить» [11].

Проведенный качественный анализ публикаций в базах научных публикаций eLibrary и Google Scholar позволил определить наиболее актуальные направления исследований по проблемам информационной безопасности в социальных сетях. Результаты анализа актуальных направлений исследований по проблемам информационной безопасности в социальных сетях отражены в таблица 1.

Таблица 1

Актуальные направления исследований по проблемам информационной безопасности в социальных сетях

Table 1. Current areas of research on information security issues in social networks

Проблемы информационной безопасности в социальных сетях	Авторы публикаций, посвященных данной проблеме
Проблема защищенности персональных данных в социальных сетях	Лосяков А. В., Слесарев Ю. В. [12], Филиппов П. Б. [13], Апатова Н. В., Минабилева М. Н. [14]
Проблема защищенности пользователей от атак социальной инженерии в социальных сетях	Фомина Н. А. [15], Дьяков Н. В. [16], Замолоцких В. С., Сидоренко В. Г. [17]
Проблема фишинга в социальных сетях	Кудрявцев О. А., Щекочихин О. В. [18], Аникина Н. А., Соколов Н. А. [19], Нилин П. А., Чугунова О. В. [20]

Проблема защищенности персональных данных в социальных сетях. В исследовании Лосякова А. В. и Слесарева Ю. В. [12] рассматриваются вопросы правового регулирования размещения и защиты персональных данных в социальных сетях. В частности, авторы выделяют следующие правовые проблемы в сфере защиты персональных данных: «отсутствие четких формулировок понятия «персональные данные»; отсутствие выстроенного правового механизма применения законодательства к нарушителям; неопределенность в методах и пределах правового регулирования в сфере использования социальных сетей» [12]. Согласно Федеральному закону от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [21], «персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [21]. При этом в законе отмечается, что «обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных» [21].

В своей работе Филиппов Б. П. [13] рассматривает вопросы использования и реализации защиты персональных данных в социальных сетях. Автор акцентирует внимание на том, что «социальные сети позволяют совместно использовать, сравнивать и объединять отдельные базы данных, в том числе размещенные в них персональные данные, что может привести к непредсказуемым последствиям, в частности, данные, размещенные по воле пользователей, могут нести опасность, поскольку являются объектами для атак с целью кражи конфиденциальных данных или их отправки киберпреступникам» [13]. Автор исследования указывает на существующие программные реализации безопасности в социальных сетях, которые помогают задать уровень открытости для коммуникации в социальных сетях, а также на возможности агентской организации безопасности в социальных сетях средствами родительского контроля, которые могут использоваться для повышения уровня информационной безопасности в социальных сетях как для несовершеннолетних пользователей социальных сетей, так и для сотрудников компаний с целью их ограничения в тратах рабочего времени в социальных сетях, а также для предотвращения утечки конфиденциальной информации, которую сотрудник может допустить через переписку или разглашение на страницах социальной сети случайно или намеренно.

Апатова Н. В. и Минабилева М. Н. в своем исследовании [14] выделяют такие риски безопасности персональных данных в социальных сетях, как атаки с использованием вредоносных программ (программы-вымогатели); атаки с применением методов социальной инженерии (фишинг); использование сторонних приложений для социальных сетей, что может привести к риску кражи пароля от ученой записи аккаунта социальной сети.

Проблема защищенности пользователей от атак социальной инженерии в социальных сетях. Фомина Н. А. в своем исследовании [15] освещает проблему использования методов социальной инженерии при мошенничестве в социальных сетях. В частности, она указывает на то, что мошенничество в социальных сетях прежде всего нацелено на «взлом страницы в социальной сети и отправку сообщений от его имени с просьбой о помощи; сбор денег на помощь «близким»; отправка зараженных файлов; получение предоплаты за покупку товара; распространение вредоносных приложений и сервисов; предложения «легкого» дополнительного заработка и т. п.» [15].

Дьяков Н. А. в своей работе [16] рассматривает виды и формы социальной инженерии, различные способы мошенничества в социальных сетях. Автор исследования также указывает, что основная часть мошеннических действий нацелена на получение денежных средств. Для того чтобы обезопасить себя при использовании социальных сетей, Дьяков Н. А. предлагает соблюдать следующие правила: «не оставлять свои персональные данные на открытых ресурсах; не откликаться на заманчивые предложения;

при получении сообщения о блокировке аккаунта не вводить данные во вложенные формы; сравните адрес, с которого пришло письмо, с адресом, с которого приходили сообщения от сети ранее; после загрузки страницы обязательно проверить наличие защищенного соединения; если вы стали получать подозрительные письма и сообщения от ваших друзей, постараться связаться с ними другим способом» [16].

В своем исследовании Замолоцких В. С. и Сидоренко В. Г. [17] рассматривают киберугрозы в социальных сетях. В качестве таких угроз авторы выделяют спам-атаки, а также атаки с применением методов социальной инженерии, в частности, фишинговые атаки, направленные на получение доступа к учетной записи пользователя социальной сети, и выделяют следующие стратегии проведения подобных атак: «уязвимость протокола WEP (метод, основанный на взломе ключей шифрования для защиты беспроводных сетей), метод полного перебора (перебор возможных комбинаций паролей к аккаунту социальной сети), метод подмены (метод, характерный маскировкой фишингового сайта под страницу входа на сайт социальной сети)» [17].

Проблема фишинга в социальных сетях. Кудрявцев О. А. и Щекочихин О. В. в своей работе [18] рассматривают особенности фишинговых атак в различных сервисах, в том числе в социальных сетях. Под фишингом авторы понимают «массовую рассылку электронных писем или сообщений для того, чтобы заманить пользователя на web-сайты, которые внешне очень похожи на обычные web-сайты различных фирм и банков, но контролируются мошенниками» [18]. При этом авторы обращают внимание на то, что атаки социальной инженерии с использованием фишинга реализуются посредством рассылки писем по электронной почте, но также они могут осуществляться и посредством отправки SMS-сообщений и сообщений в мессенджерах, а также при помощи диалогов социальных сетей. В частности, фишинг в социальных сетях усложняется тем, что перед тем, как начать рассылку вредоносных сообщений пользователям социальной сети, злоумышленнику необходимо получить доступ к аккаунту одного из пользователей. При таких атаках злоумышленники могут просить у друзей пользователя, страница которого была взломана, денег взаймы, либо отправляют ссылку на вредоносные ресурсы.

Аникина Н. А. и Соколов Н. А. в своем исследовании [19] описывают фишинг как один из самых распространенных и опасных видов онлайн-мошенничества. Успешные фишинговые атаки могут иметь серьезные последствия для жертв. Пользователи могут потерять доступ к своим аккаунтам, стать жертвами финансового мошенничества, а их личные данные могут быть использованы для преступных целей. Для защиты от фишинговых атак авторы предлагают ряд методов и средств, таких как «обучение пользователей социальных сетей признакам фишинга, использование антивирусных программ и браузеров с защитой от фишинга, аккуратность при клике на ссылки и проверке адресов веб-сайтов» [19].

Нилин П. А. и Чугунова О. В. в своем исследовании [20] описывают способы борьбы с фишинг-атаками. Для защиты от фишинга они предлагают программные решения для автоматического обнаружения и предотвращения фишинговых атак. В частности, «чтобы предотвратить фишинговые атаки, вводится дополнительный уровень безопасности при входе пользователя на веб-сайт. Он обеспечивается посредством двухфакторной аутентификации, которая представляет собой процесс подтверждения личности пользователя перед тем, как ему будет предоставлен доступ к своей учетной записи на веб-сайте. Когда пользователь ввел имя пользователя и пароль для входа в личный кабинет, проверочный код будет отправлен на зарегистрированный номер мобильного телефона пользователя по SMS. Затем необходимо ввести проверочный код для того, чтобы успешно войти в свою учетную запись» [20].

Важным элементом атак социальной инженерии с использованием фишинга в

социальных сетях является метод претекстинга. Претекстинг – это метод социальной инженерии, при котором «злоумышленник по заранее подготовленному сценарию (претекст) подводит потенциальную жертву к тому, чтобы она совершила требуемые действия или выдала необходимую конфиденциальную информацию (как правило, это осуществляется через социальные сети, телефон, электронную почту и требует предварительной обработки информации о жертве)» [22].

Данный метод социальной инженерии чаще всего реализуется посредством телефонной связи. Согласно опросу Всероссийского центра изучения общественного мнения (ВЦИОМ) [23], проведенного в феврале 2024 года, 67 % россиян за последние полгода-год получали звонки от телефонных мошенников, что на 10 % больше, чем в 2021 году. Согласно результатам исследования Зотиной Е. В., «материалы следственно-судебной практики, сведения из Интернет-источников содержат такие примеры реализации претекстинга в рамках телефонного мошенничества, как «Банковская карта заблокирована», «Родственник попал в ДТП», «Получение компенсации за БАД», «Выигрыш в лотерее», «Банковский счет заблокирован в связи с попыткой нелегального перевода в недружественную страну» (последний пример связан с интенсификацией мошеннических действий в связи с проведением специальной военной операции)» [24], причем сценарии «Банковская карта заблокирована» и «Родственник попал в ДТП» являются одними из самых распространенных сценариев претекстинга в рамках телефонного мошенничества. Согласно отчету Verizon 2023 Data Breach Investigations Report [25], представленного компанией Verizon Business, атаки с использованием претекстинга в 2023 году составляли более 50 % всех атак с использованием методов социальной инженерии».

Помимо телефонного мошенничества, претекстинг получил широкое распространение при проведении атак социальной инженерии в социальных сетях. Исследование, проведенное компанией Positive Technologies [26], показывает, что социальные сети являются одним из самых распространенных каналов для атак социальной инженерии, ключевым элементом которых являются техники фишинга и претекстинга. В таблице 2 представлена сравнительная характеристика атак социальной инженерии с использованием техники претекстинга по телефону и в социальных сетях.

Таблица 2

Сравнительная характеристика атак социальной инженерии
с использованием техники претекстинга по телефону и в социальных сетях

Table 2. Comparative characteristics of social engineering attacks using pretexting techniques over the phone and on social networks

Критерий	Претекстинг по телефону	Претекстинг в социальной сети
Вредоносное воздействие	Атака социальной инженерии с использованием техники претекстинга по телефону	Атака социальной инженерии с использованием претекстинга в социальной сети
Источник угрозы	Мобильный телефон	Социальная сеть
Уязвимость	Телефонный звонок злоумышленника потенциальной жертве	Отправка сообщения в социальной сети злоумышленником потенциальной жертве
Объект воздействия	Пользователь мобильного телефона	Пользователь социальной сети
Способ реализации угрозы	Техника претекстинга	

Проведенный анализ публикаций по проблемам противодействия методам социальной инженерии в социальных сетях демонстрирует возрастающий интерес ученых к данной области исследований. В рамках контент-анализа публикаций в базах научных публикаций eLibrary, Scopus, Google Scholar за последние 10 лет были подобраны ключевые слова, которые описывают тематику публикаций по соответствующей области

исследований. В качестве основы комбинаций для поисковых запросов использовались комбинации ключевого слова «социальные сети / social networks» со следующим набором ключевых слов: «социальная инженерия / social engineering», «социоинженерные атаки / social engineering attacks», «защита информации / data protection / information protection», «информационная безопасность / information security».

На рисунке 1 представлены количественные результаты публикационной активности по теме исследования за последние 10 лет (с 2014 по 2023 гг.), которые показывают рост публикаций по проблемам противодействия методам социальной инженерии в социальных сетях.

Рис. 1. Результаты публикационной активности по проблемам противодействия методам социальной инженерии в социальных сетях в базах публикаций eLibrary, Scopus, Google Scholar за последние 10 лет (с 2014 по 2023 гг.)

Fig. 1. Results of publication activity on the problems of countering social engineering methods in social networks in the publication databases Library, Scopus, Google Scholar over the past 10 years (from 2014 to 2023)

Проведенный анализ публикаций по проблеме претекстинга как метода социальной инженерии также демонстрирует возрастающий интерес ученых к данной области исследований. На рисунке 2 представлены количественные результаты публикационной активности по ключевому слову «претекстинг» за последние 10 лет (с 2014 по 2023 гг.), которые показывают рост публикаций по проблеме претекстинга.

При этом следует отметить, что исследований, посвященных проблеме претекстинга в социальных сетях (публикации, содержащие ключевые слова «претекстинг / pretexting», «социальные сети / social media»), выявлено недостаточно (рис. 3).

Таким образом, атаки социальной инженерии с использованием претекстинга в социальных сетях являются серьезной угрозой информационной безопасности для пользователей социальных сетей. В связи с этим следует отметить, что социальные сети являются одной из основных площадок для коммуникации и обмена информацией как в России, так и во всем мире. Месячный охват самых популярных социальных сетей в Российской Федерации (ВКонтакте, Telegram) составляет более 80 миллионов пользователей, что делает их более привлекательными для злоумышленников.

Исследования, посвященные проблемам информационной безопасности в социальных сетях, становятся более актуальными. Одной из актуальных проблем, с которыми сталкиваются пользователи социальных сетей, является проблема защищенности пользователей от атак использованием социальной инженерии, в том чисел с использованием техники фишинга и претекстинга. Следует отметить, что в последние годы наблюдается рост числа исследований, посвященных изучению претекстинга как мето-

да социальной инженерии. Однако количество исследований, посвященных проблеме претекстинга в социальных сетях, остается недостаточным.

Рис. 2. Результаты публикационной активности по ключевому слову «претекстинг / pretexting» в базах публикаций eLibrary, Scopus, Google Scholar, за последние 10 лет (с 2014 по 2023 гг.)

Fig. 2. Results of publication activity for the keyword “pretexting” in the publication databases eLibrary, Scopus, Google Scholar, over the past 10 years (from 2014 to 2023)

Рис. 3. Результаты публикационной активности по комбинации ключевых слов «социальные сети / social media» и «претекстинг / pretexting» в базах публикаций eLibrary, Scopus, Google Scholar за последние 10 лет (с 2014 по 2023 гг.)

Fig. 3. Results of publication activity for the combination of keywords “social networks / social media” and “pretexting” in the publication databases eLibrary, Scopus, Google Scholar over the past 10 years (from 2014 to 2023)

Опасность претекстинга как метода социальной инженерии неоспорима. С использованием техники претекстинга злоумышленники могут получить доступ к персональным данным, конфиденциальной информации, а также к денежным средствам своих жертв. Кроме того, претекстинг может быть комбинирован с другими методами социальной инженерии, в частности с фишингом, что делает такие атаки еще более опасными.

Следовательно, в целях противодействия атакам социальной инженерии в социальных сетях с использованием претекстинга необходимо разработать модели и методики противодействия соответствующим атакам. При этом одним из возможных подходов является обучение пользователей социальных сетей основам безопасности в социальных сетях и выявлению атак социальной инженерии с использованием претек-

стинга. Это может быть достигнуто путем проведения информационных кампаний, разработки обучающих материалов и тренировочных сценариев, которые помогут пользователям социальных сетей распознавать атаки социальной инженерии с использованием претекстинга и принимать соответствующие меры для предотвращения подобных атак.

Таким образом, проблема претекстинга в социальных сетях является актуальной и требует дальнейших исследований. Разработка обучающих систем, направленных на повышение осведомленности пользователей социальных сетей о социоинженерных атаках с использованием претекстинга, а также разработка эффективных алгоритмов обнаружения таких атак являются перспективными направлениями исследований в области информационной безопасности социальных сетей.

Примечания

1. Ветцель К. Я. Социальные медиа и социальные сети: проблемы терминологии и модели взаимодействия пользователей // Международный научно-исследовательский журнал. 2020. № 9-1 (99). С. 139–141. DOI: 10.23670/IRJ.2020.99.9.023

2. Брославский П. В., Полянский С. С. Роль социальных сетей в формировании информационного общества // Высокие технологии, наука и образование : актуальные вопросы, достижения и инновации : сб. ст. VII Всерос. науч.-практ. конф., Пенза, 27 июня 2020 года. Пенза : Наука и Просвещение, 2020. С. 229–231.

3. Абдуллаева Р. А. Анализ влияния социальных сетей на жизнь современного общества // Международный журнал прикладных и фундаментальных исследований. 2015. № 9-3. С. 542–546. URL: https://applied-research.ru/ru/article/view?id=7369 (дата обращения: 17.03.2024).

4. Иванько А. Ф., Иванько М. А., Лихтина Е. К. Социальные сети, как элемент информационных технологий // Научное обозрение. Фундаментальные и прикладные исследования. 2020. № 1. С. 5. URL: https://scientificreview.ru/ru/article/view?id=77 (дата обращения: 18.03.2024).

5. Табашникова К. С., Яговцева А. А. Социальные сети как инструмент продвижения бизнеса на территории Российской Федерации в реалиях 2023 года // Молодой ученый. 2023. № 4 (451). С. 436–438. URL: https://moluch.ru/archive/451/99462/ (дата обращения: 22.03.2024).

6. Digital 2024: Global Overview Report // DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 02.04.2024).

7. Biggest social media platforms 2024 // Statista – The Statistics Portal for Market Data, Market Research and Market Studies. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (дата обращения: 28.03.2024).

8. Mediascope – Рейтинги // Исследовательская компания Mediascope.
URL: https://mediascope.net/data/ (дата обращения: 03.04.2024).

9. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // КонсультантПлюс : сайт.
URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 24.03.2024).

10. Митник К. Д., Саймон В. Л. Искусство обмана. Компания АйТи, 2004. 360 с.

11. Хэднеги К. Искусство обмана: Социальная инженерия в мошеннических схемах. Москва : Альпина Паблишер, 2020. 430 с.

12. Лосяков А. В., Слесарев Ю. В. Правовое регулирование размещения и защиты персональных данных в социальных сетях // XXI век: итоги прошлого и проблемы настоящего плюс. 2016. № 4 (32). С. 143–147.

13. Филиппов П. Б. Использование и реализация защиты персональных данных в социальных сетях Интернета // Прикладная информатика. 2012. № 2 (38). С. 71–77.

14. Апатова Н. В., Минабилева М. Н. Проблемы безопасности данных в социальных сетях // Проблемы информационной безопасности социально-экономических систем : VII Всерос. с междунар. участием науч.-практ. конф., Гурзуф, 18–20 февраля 2021 года. Симферополь : Крымский федеральный университет им. В. И. Вернадского, 2021. С. 100–101.

15. Фомина Н. А. Использование методов социальной инженерии при мошенничестве в социальных сетях // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи : материалы внутривузовской конф., Магнитогорск, 09–12 октября 2015 года / под ред. Г. Н. Чусавитиной, Е. В. Черновой, О. Л. Колобовой. Магнитогорск : Магнитогорский гос. тех. ун-т им. Г. И. Носова, 2015. С. 443–453.

16. Дьяков Н. В. Применение методов социальной инженерии в социальных сетях // Общество. 2020. № 2 (17). С. 126–128.

17. Замолоцких В. С., Сидоренко В. Г. Киберугрозы в социальных сетях // Информатизация образования и науки. 2020. № 4 (48). С. 66–75.

18. Кудрявцев О. А., Щекочихин О. В. Фишинг в электронной почте, sms-сообщениях, мессен-

джерах и социальных сетях // Поведение молодежи в современном Интернет-пространстве: стратегии, риски, защита : сб. ст. Всерос. студенческой науч.-практ. конф., Орехово-Зуево, 15 мая 2018 года. Орехово-Зуево : Гос. гуманит.-технол. ун-т, 2018. С. 22–26.

19. Аникина Н. А., Соколов Н. А. Фишинг и мошенничество в настоящее время // Территория науки и образования. 2024. № 1. С. 85–87.

20. Нилин П. А., Чугунова О. В. Исследование способов борьбы с фишинг-атаками // Инновации в информационных технологиях, машиностроении и автотранспорте (ИИТМА-2020) : сб. материалов IV Междунар. науч.-практ. конф. с онлайн-участием, Кемерово, 07–10 декабря 2020 года. Кемерово : Кузбасский гос. тех. ун-т им. Т. Ф. Горбачева, 2020. С. 89–91.

21. О персональных данных : Федеральный закон от 27.07.2006 N 152-ФЗ (последняя редакция) // СПС КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 01.04.2024).

22. Захлевная И. И. Социальная инженерия: актуальная угроза и меры защиты // Международная научно-техническая конференция молодых ученых БГТУ им. В. Г. Шухова, посвященная 170-летию со дня рождения В. Г. Шухова, Белгород, 16–17 мая 2023 года : сб. докл. Белгород : Белгородский гос. технол. ун-т им. В. Г. Шухова, 2023. Ч. 17. С. 409–412.

23. Телефонное мошенничество : мониторинг // ВЦИОМ. Новости.
URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 26.03.2024).

24. Зотина Е. В. Антропология телефонного мошенничества с использованием претекстинга : криминологическое исследование // Мониторинг правоприменения. 2023. № 2 (47). С. 32–38.
DOI: 10.21681/2226-0692-2023-2-32-38

25. Verizon 2023 Data Breach Investigations Report // Verizon.
URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 24.03.2024).

26. Cybersecurity threatscape: Q3 2023 // Positive Technologies.
URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения: 23.03.2024).

References

1. Wetzel K. Ya. Social media and social networks: problems of terminology and models of user interaction // International Scientific Research Journal. 2020. No. 9-1 (99). P. 139–141. DOI: 10.23670/IRJ.2020.99.9.023

2. Broslavsky P. V., Polyansky S. S. The role of social networks in the formation of the information society // High technologies, science and education: current issues, achievements and innovations : collection of articles of the 7th All-Russian Scientific and Practical Conference, Penza, June 27, 2020. Penza : Science and Enlightenment, 2020. P. 229–231.

3. Abdullaeva R. A. Analysis of the influence of social networks on the life of modern society // International Journal of Applied and Fundamental Research. 2015. No. 9-3. P. 542–546. URL: https://applied-research.ru/ru/article/view?id=7369 (access date: 17/03/2024).

4. Ivanko A. F., Ivanko M. A., Likhtina E. K. Social networks as an element of information technology // Scientific Review. Basic and applied research. 2020. No. 1. P. 5.
URL: https://scientificreview.ru/ru/article/view?id=77 (access date: 18/03/2024).

5. Tabashnikova K. S., Yagovtseva A. A. Social networks as a tool for promoting business on the territory of the Russian Federation in the realities of 2023 // Young Scientist. 2023. No. 4 (451). P. 436–438. URL: https://moluch.ru/archive/451/99462/ (access date: 22/03/2024).

6. Digital 2024: Global Overview Report // DataReportal – Global Digital Insights. URL: https://datareportal.com/reports/digital-2024-global-overview-report (access date: 02/04/2024).

7. Biggest social media platforms 2024 // Statista – The Statistics Portal for Market Data, Market Research and Market Studies. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (access date: 28/03/2024).

8. Mediascope – Рейтинги // Исследовательская компания Mediascope.
URL: https://mediascope.net/data/ (access date: 03/04/2024).

9. On approval of the Information Security Doctrine of the Russian Federation : Decree of the President of the Russian Federation dated December 5, 2016 No. 646 // ConsultantPlus : site.
URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (access date: 24/03/2024).

10. Mitnik K. D., Simon V. L. The art of deception. IT Co, 2004. 360 p.

11. Hadnegy K. The art of deception: Social engineering in fraudulent schemes. Moscow : Alpina Publisher, 2020. 430 p.

12. Losyakov A. V., Slesarev Yu. V. Legal regulation of placement and protection of personal data in social networks // 21th Century: Results of the Past and Problems of the Present Plus. 2016. No. 4 (32). P. 143–147.

13. Filippov P. B. Use and implementation of personal data protection in social networks of the Internet // Applied Informatics. 2012. No. 2 (38). P. 71–77.

14. Apatova N. V., Minabileva M. N. Problems of data security in social networks // Problems of information security of socio-economic systems : 7th All-Russian scientific and practical conference with international participation, Gurzuf, February 18–20, 2021. P. 100–101.

15. Fomina N. A. The use of social engineering methods in fraud on social networks // Information security and issues of preventing cyber extremism among youth : Proceedings of the intra-university conference, Magnitogorsk, October 09–12, 2015 / Edited by G. N. Chusavitina, E. V. Chernova, O. L. Kolobova. Magnitogorsk : Magnitogorsk State Technical University named after G. I. Nosov, 2015. P. 443–453.

16. Dyakov N. V. Application of social engineering methods in social networks // Society. 2020. No. 2 (17). P. 126–128.

17. Zamolotskikh V. S., Sidorenko V. G. Cyber threats in social networks // Informatization of Education and Science. 2020. No. 4 (48). P. 66–75.

18. Kudryavtsev O. A., Shchekochikhin O. V. Phishing in email, SMS messages, instant messengers and social networks // Youth behavior in the modern Internet space: strategies, risks, protection: collection of articles of the All-Russian Student Scientific and Practical Conference, Orekhovo-Zuevo, May 15, 2018. Orekhovo-Zuevo : State University of Humanities and Technology, 2018. P. 22–26.

19. Anikina N. A., Sokolov N. A. Phishing and fraud at the present time // Territory of Science and Education. 2024. No. 1. P. 85–87.

20. Nilin P. A., Chugunova O. V. Research on ways to combat phishing attacks // Innovations in information technologies, mechanical engineering and motor transport (IITMA-2020) : collection of materials of the 4th International scientific and practical conference with online participation, Kemerovo, December 07–10, 2020. Kemerovo : Kuzbass State Technical University named after T. F. Gorbachev, 2020. P. 89–91.

21. On Personal Data : Federal Law, dated July 27, 2006 N 152-FZ (latest edition) // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (access date: 01/04/2024).

22. Zakhlevnaya I. I. Social engineering: current threat and protective measures // International scientific and technical conference of young scientists of BSTU named after V. G. Shukhov, dedicated to the 170th anniversary of the birth of V. G. Shukhov, Belgorod, May 16–17, 2023 : Collection of reports. Belgorod : Belgorod State Technological University named after V. G. Shukhov, 2023. Part 17. P. 409–412.

23. Telephone fraud : monitoring // VTsIOM. News. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (access date: 26/03/2024).

24. Zotina E. V. Anthropology of telephone fraud using pretexting : criminological research // Law Enforcement Monitoring. 2023. No. 2 (47). P. 32–38. DOI: 10.21681/2226-0692-2023-2-32-38

25. Verizon 2023 Data Breach Investigations Report // Verizon.
URL: https://www.verizon.com/business/resources/reports/dbir/ (access date: 24/03/2024).

26. Cybersecurity threatscape: Q3 2023 // Positive Technologies.
URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/ (access date: 23/03/2024).

Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 14.04.2024; *одобрена после рецензирования 29.04.2024*; *принята к публикации 30.04.2024.*

The authors declare no conflicts of interests.

The article was submitted 14.04.2024; *approved after reviewing 29.04.2024*; *accepted for publication 30.04.2024.*