Афонина Виктория Владимировна
студентка 4 курса бакалавриата, группа ИБ23-6,
факультет Информационных технологий и анализа больших данных, кафедра Информационной безопасности,
Финансовый университет при Правительстве Российской Федерации, Москва

Крепак Иван Павлович
руководитель Группы информационной безопасности, ООО «Клиника Будь Здоров», студент 3 курса аспирантуры, группа ИБ24-1а,
факультет Информационных технологий и анализа больших данных, кафедра Информационной безопасности,

ОЦЕНКА ЗАЩИЩЁННОСТИ УЧЁТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ: АНАЛИЗ НАСТРОЕК ПРИВАТНОСТИ, ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ТИПОВЫХ ОШИБОК

Аннотация

В данной научной статье рассматривается проблема защищённости учётных записей пользователей социальных сетей. Даётся общая характеристика угроз, которым подвергаются аккаунты в социальных сетях, приводится обзор резонансных инцидентов утечки данных [1 - 3] «Facebook*», «ВКонтакте» и «MOAB» и статистика инцидентов информационной безопасности в российском Интернет-пространстве за 2024 и 2025 годы [4]. Далее, в статье последовательно анализируются три ключевых фактора защищённости учётной записи - настройки приватности профиля, двухфакторная аутентификация (2FA) и типовые поведенческие ошибки пользователей для 2FA и для классификации ошибок приведены сравнительные таблицы. Оценка построена на данных отраслевых исследований «Microsoft», Роскомнадзора и независимых аналитических

центров по кибербезопасности [4 - 6]. В заключение статьи предлагается комплекс практических рекомендаций по повышению защищённости учётных записей в социальных сетях. Отдельное внимание уделяется распространённым заблуждениям пользователей относительно достаточности базовой защиты и роли платформ в информировании о рисках. Материал может быть полезен как рядовым пользователям социальных сетей, так и специалистам по информационной безопасности, разрабатывающим программы повышения цифровой грамотности. Полученные выводы подчёркивают необходимость сочетания технических и поведенческих мер защиты для устойчивого снижения рисков компрометации учётных записей.

Ключевые слова: защищённость учётной записи, социальная сеть, приватность в Интернете, двухфакторная аутентификация, SSO, утечка персональных данных, цифровая грамотность, поведенческий анализ, несанкционированный доступ, перехват сообщений.

Assessment of social media user account security: analysis of privacy settings, two-factor authentication and typical mistakes

Afonina Viktoriya Vladimirovna
4th year undergraduate student, group IB23-6,
Faculty of Information Technology and Big Data Analysis,
Department of Information Security,
Financial University under the Government of the Russian Federation, Moscow
237577@edu.fa.ru

Krepak Ivan Pavlovich
head of Information security group, «Klinika Bud Zdorov» LLC,
post-graduate student, 3rd year, IB24-1a,
Faculty of Information Technology and Big Data Analysis,

Department of Information Security,
Financial University under the Government of the Russian Federation, Moscow
krepak.2311@yandex.ru

Abstract

This article examines the problem of social media user account security. A general characterization of the threats faced by social network accounts is given, along with an overview of high-profile data breach incidents [1 - 3] with «Facebook*», «VKontakte» and «MOAB») [1, 2, 3] and Russian statistics for 2024–2025 [4]. The article then successively analyzes three key factors of account security - profile privacy settings, two-factor authentication (2FA), and typical user behavioral mistakes; comparative tables are provided for 2FA methods and for the classification of mistakes. The assessment is based on industry data from «Microsoft», Roskomnadzor, and independent cybersecurity analytics centers [4 - 6]. In conclusion, the article offers a set of practical recommendations for improving social media account security. Special attention is paid to common user misconceptions about the sufficiency of basic protection measures and to the role platforms play in informing users about risks. The material may be useful both for ordinary social media users and for information security specialists developing digital literacy programs. The findings highlight the need to combine technical and behavioral protective measures to achieve a sustained reduction in the risk of account compromise.

Keywords: account security, social network, online privacy, two-factor authentication, SSO, personal data leak, digital literacy, behavioral analysis, unauthorized access, message interception

Введение

Социальные сети перестали быть исключительно площадкой для общения и превратились в информационную инфраструктуру, через которую пользователи хранят личные фотографии, ведут переписку, совершают

платежи и авторизуются в сторонних сервисах через единый «Single Sign-On»-вход. Из-за этого, учётная запись в социальной сети фактически становится цифровым эквивалентом паспорта и кошелька одновременно, а её компрометация влечёт за собой не только репутационный, но и финансовый ущерб для владельца.

Актуальность темы обусловлена устойчивым ростом числа утечек персональных данных и одновременно низким уровнем цифровой грамотности пользователей: значительная часть аккаунтов остаётся уязвимой не из-за отсутствия технических средств защиты, а из-за того, что эти средства либо не эксплуатируются, либо применяются некорректно. Целью данной научной статьи является системная оценка защищённости учётной записи пользователя социальной сети через анализ трёх взаимосвязанных факторов: настроек приватности профиля, применения двухфакторной аутентификации и типовых поведенческих ошибок. Объектом исследования выступает учётная запись пользователя социальной сети как объект защиты, предметом - совокупность технических настроек и пользовательских практик, определяющих уровень её защищённости. Для достижения поставленной цели решаются следующие задачи: охарактеризовать основные угрозы для учётных записей, рассмотреть резонансные инциденты утечек как эмпирическую иллюстрацию проблемы, проанализировать эффективность и ограничения настроек приватности и двухфакторной аутентификации, классифицировать типовые ошибки пользователей и сформулировать практические рекомендации.

1. Теоретические основы и обзор угроз для учётных записей социальных сетей

1.1 Понятие защищённости учётной записи

Под защищённостью учётной записи в данной статье понимается способность аккаунта пользователя противостоять попыткам несанкционированного доступа, а также минимизировать ущерб в случае попытки такового события. Защищённость аккаунта не сводится к одному

техническому механизму, а формируется совокупностью факторов: техническими настройками, предоставляемыми платформой (приватность, двухфакторная аутентификация, уведомления о входе), и интеракцией самого пользователя (выбор паролей, реакция на подозрительную активность, отношение к фишинг сообщениям). Текущий комплексный подход соответствует принятой в информационной безопасности модели «человек - процесс - технология», согласно которой устойчивость системы определяется наиболее слабым из этих трёх звеньев.

1.2 Классификация угроз

Среди основных угроз для учётных записей пользователей социальных сетей можно выделить следующие группы. Во-первых, подбор и перебор паролей – «брутфорс» и «credential stuffing», при котором злоумышленник проверяет пароли из ранее утёкших баз данных на других сервисах, рассчитывая на повторное использование пароля пользователем [13]. Во-вторых, фишинг атаки, направленные на кражу учётных данных под видом официальных уведомлений платформы или писем от знакомых контактов. В-третьих, перехват сессии и SIM-свопинг - переоформление номера телефона жертвы на SIM-карту злоумышленника с целью перехвата SMS-кодов подтверждения [14]. В-четвёртых, социальная инженерия, эксплуатирующая доверие пользователя к знакомым лицам или авторитетным источникам. Индикаторами компрометации аккаунта обычно считаются вход с незнакомого устройства или из другого региона, попытка смены пароля без участия владельца, рассылка сообщений от его имени, а также массовые подписки или отписки за короткий промежуток времени.

1.3 Обзор резонансных инцидентов информационной безопасности

Масштаб проблемы наглядно иллюстрируют крупные инциденты последних лет. В 2016 году в открытом доступе оказалась база данных социальной сети «ВКонтакте», содержащая свыше 100,5 млн записей (имена, адреса электронной почты, номера телефонов и пароли пользователей). Анализ базы показал, что самым распространённым паролем являлся

«123456», встречавшийся более 709 тысяч раз, а среди других популярных вариантов оказались «qwerty» и «123123» [1]. Данный случай демонстрирует, что даже спустя годы после утечки простые и предсказуемые пароли остаются массовым явлением.

В апреле 2021 года на хакерском форуме в открытом доступе оказались персональные данные более 533 млн пользователей «Facebook*» из 106 стран, включая номера телефонов, полные имена, даты рождения и биографические сведения; по данным издания Business Insider, база была собрана методом веб-скрейпинга через уязвимость функции импорта контактов, устранённую платформой ещё в 2019 году [2]. Инцидент показал, что даже устранённая техническая уязвимость может годами создавать риск для пользователей, чьи данные уже были собраны.

В январе 2024 года стало известно о «MOAB» («Mother of All Breaches») - компиляции объёмом 12 ТБ и порядка 26 млрд записей, объединившей данные пользователей множества платформ, включая около 101 млн записей «ВКонтакте» и 41 млн записей Telegram. Исследователи отметили, что подобные компиляции особенно опасны из-за массового повторного использования одних и тех же учётных данных пользователями на разных сервисах [3]. По данным Роскомнадзора, в течение 2024 года в России было зафиксировано 135 подтверждённых утечек персональных данных, содержащих более 710 млн записей, а суммарный объём скомпрометированных данных за три предшествующих года превысил 4,5 млрд записей [4]. Указанные примеры подтверждают, что проблема защищённости учётных записей носит не гипотетический, а системный и постоянно воспроизводящийся характер.

2. Анализ настроек приватности профиля

2.1 Роль настроек приватности как первого рубежа защиты

Настройки приватности определяют объём информации, доступной посторонним пользователям, и напрямую влияют на то, какими данными может воспользоваться злоумышленник при подготовке целевой атаки. Чем

больше персональной информации доступно публично - дата рождения, номер телефона, геолокация, список друзей, место работы, тем проще злоумышленнику составить достоверный сценарий социальной инженерии или подобрать контрольные вопросы для восстановления доступа к аккаунту. Открытые настройки приватности также увеличивают цифровую поверхность атаки: чем больше метаданных доступно, тем выше вероятность формирования цифрового профиля жертвы, который впоследствии может эксплуатироваться для таргетированного мошенничества или травли.

2.2 Сравнительный аспект и практические ограничения

Практика показывает, что пользователи склонны недооценивать связь между открытостью профиля и риском компрометации: настройки приватности часто воспринимаются как инструмент защиты от нежелательного социального внимания, а не как элемент защиты от целенаправленной компьютерной атаки [15]. Между тем, именно общедоступные персональные данные - номер телефона, дата рождения, наименование юридического лица работодателя, чаще всего используются злоумышленниками при попытке пройти процедуру восстановления пароля или составить убедительное фишинг сообщение, имитирующее обращение от имени коллеги или знакомого. Таким образом, ограничение видимости профиля и контроль над тем, кто может видеть публикации, список друзей и контактные данные, является базовым, но зачастую недооценённым уровнем защиты учётной записи.

3. Анализ двухфакторной аутентификации

3.1 Принцип работы и статистика эффективности

Двухфакторная аутентификация (2FA) добавляет второй независимый фактор подтверждения личности - одноразовый код, push-уведомление или аппаратный ключ (в дополнение к паролю). По данным исследования, представленного инженерами Microsoft на конференции RSA в 2020 году, 99.9% скомпрометированных учётных записей на момент взлома не использовали многофакторную аутентификацию, при этом компания

ежедневно отслеживает более 30 млрд событий входа в свои системы, а в среднем около 0,5% всех учётных записей подвергаются компрометации ежемесячно [5]. В том же исследовании отмечалось, что порядка 60% пользователей повторно используют один и тот же пароль на разных сервисах, что делает единичную утечку данных фактором риска сразу для нескольких учётных записей [5]. Более поздние отчёты Microsoft подтверждают устойчивость этой закономерности: свыше 99% успешных атак на учётные записи происходит там, где многофакторная аутентификация не была настроена [6]. Эти данные делают 2FA одним из наиболее эффективных по соотношению затрат и результата инструментов защиты учётной записи: пароль, попавший в руки злоумышленника в результате утечки, сам по себе перестаёт быть достаточным условием для входа в аккаунт.

3.2 Сравнение методов двухфакторной аутентификации

Эффективность 2FA существенно зависит от выбранного способа подтверждения второго фактора. Основные варианты и их характеристики раскрыты в Таблице 1.

2FA-метод	**Принцип работы**	**Ключевые риски**	**Уровень надёжности**
SMS-код	Одноразовый код направляется на привязанный номер телефона	Перехват сообщений, SIM-свопинг, зависимость от сотовой сети	Низкий / средний
Push-уведомление	Подтверждение входа во встроенном приложении платформы	Риск случайного или усталостного одобрения запроса (MFA fatigue)	Средний

2FA-метод	Принцип работы	Ключевые риски	Уровень надёжности
Приложение-аутентификатор (TOTP)	Временный код генерируется на устройстве по криптографическому алгоритму	Требует наличия устройства, риск при потере без резервных кодов	Высокий
Аппаратный FIDO2/U2F-ключ	Физическое устройство подтверждает вход криптографической подписью	Риск физической утери ключа	Очень высокий

Таблица 1. Сравнение методов двухфакторной аутентификации.

3.3 Ограничения двухфакторной аутентификации

Несмотря на высокую статистическую эффективность, 2FA не является абсолютной защитой. Против целенаправленных атак с применением социальной инженерии, поддельных страниц авторизации (фишинг в реальном времени, перехватывающий пароу логина и пароля) или перехвата активной сессии через кражу cookie-файлов, данный механизм может оказаться недостаточным. Кроме того, распространение push-уведомлений способствовало появлению нового вектора атаки, который называется «MFA fatigue». Он работает следующим образом. Злоумышленник, уже завладевший паролем, отправляет жертве множественные запросы на подтверждение входа в расчёте на то, что она одобрит один из них по невнимательности или физической усталости. Из этого следует, что 2FA должна рассматриваться как необходимый, но не единственный элемент комплексной защиты учётной записи, а наиболее устойчивыми к атакам являются методы, основанные на криптографических ключах, привязанных к конкретному устройству.

4. Типовые ошибки пользователей

4.1 Классификация типовых ошибок

Анализ практики компрометации учётных записей позволяет выделить несколько устойчиво повторяющихся категорий пользовательских ошибок, обозначенных в Таблице 2.

№	Категория ошибки	Индикаторы проявления	Отрицательные последствия
1	Слабые и повторяющиеся пароли	Использование простых, коротких паролей (комбинация цифр и даты) на нескольких сервисах	Credential stuffing после единичной утечки
2	Игнорирование 2FA	2FA не включена либо используется только SMS	Успешный вход по украденному паролю
3	Избыточные данные профиля	Публикация номера телефона, геометок, места работы в открытом доступе	Упрощение подготовки фишинга и социальной инженерии
4	Игнорирование уведомлений об аутентификации	Уведомления о новом устройстве остаются без внимания	Позднее обнаружение компрометации
5	Доверие к фишинг сообщениям	Переход по ссылкам на	Прямая передача пароля и 2FA-

№	Категория ошибки	Индикаторы проявления	Отрицательные последствия
		поддельные страницы авторизации	кода злоумышленнику
6	Неконтролируемый доступ сторонних приложений (в т.ч. через API)	Ранее выданные разрешения приложениям не пересматриваются	Утечка данных через скомпрометированное стороннее приложение

Таблица 2. Классификация типовых ошибок пользователей социальных сетей.

4.2 Причины устойчивости типовых ошибок

Устойчивость перечисленных ошибок объясняется не только недостатком технической грамотности, но и рядом поведенческих факторов: стремлением пользователя минимизировать когнитивную нагрузку (отсюда повторное использование простых паролей), доверием к привычному интерфейсу коммуникации (уязвимость к фишингу, имитирующему легитимные уведомления), а также игнорированием каких-либо угроз информационной безопасности, снижающим мотивацию включать дополнительные механизмы защиты. Показательно, что даже пользователи, формально использующие двухфакторную аутентификацию, нередко выбирают наименее защищённую опцию (SMS) потому, что он не требует установки дополнительного приложения. Это подтверждает, что удобство использования остаётся для большинства пользователей приоритетнее теоретической надёжности.

5. Рекомендации по повышению защищённости учётных записей

На основании проведённого анализа был сформулирован следующий комплекс рекомендаций для повышения защищённости учётной записи в социальной сети:

1. Использовать уникальный сложный пароль для каждого сервиса и менеджер паролей для их хранения, исключив повторное использование одинаковых паролей на разных платформах.

2. Включать двухфакторную аутентификацию, отдавая предпочтение приложению-аутентификатору или аппаратному ключу перед SMS-подтверждением как менее устойчивым к перехвату способом.

3. Периодически редактировать настройки приватности профиля, ограничивая видимость персональных данных (телефон, дата рождения, геометки) перечнем доверенных контактов.

4. Регулярно проверять список активных устройств, подключённых сторонних приложений и API-ключей, отзывая доступ у неиспользуемых сервисов.

5. Критически относиться к сообщениям и ссылкам, побуждающим в срочном порядке ввести пароль, код подтверждения или личные данные, даже если сообщение выглядит как легитимное уведомление платформы.

6. Своевременно реагировать на уведомления о подозрительной активности, незамедлительно редактируя пароль и завершая все активные сеансы при первых признаках компрометации.

Заключение

Проведённый анализ показывает, что защищённость учётной записи пользователя социальной сети определяется не одним техническим механизмом, а сочетанием корректно настроенной приватности профиля, применения двухфакторной аутентификации и осознанного поведения пользователя. Рассмотренные инциденты - утечка «ВКонтакте» в 2016 году [1], утечка «Facebook*» 2021 года [2] и компиляция «MOAB» 2024 года [3] - показывают, что проблема носит системный и повторяющийся характер, а её масштаб в Российском сетевом сегменте продолжает измеряться большим

количеством скомпрометированных записей ежегодно. Настройки приватности ограничивают объём данных, доступных потенциальному злоумышленнику и снижают риск успешной социальной инженерии. Двухфакторная аутентификация, по данным «Microsoft», блокирует свыше 99% автоматизированных атак [6], однако не является абсолютным решением против комплексных APT-атак, в первую очередь против фишинга в реальном времени и MFA fatigue. Типовые пользовательские ошибки – недостаточно сложные пароли, избыточная открытость профиля, игнорирование второго фактора аутентификации и доверчивость к фишингу остаются главными причинами компрометации аккаунтов даже при наличии технических средств защиты. Таким образом, повышение действительной защищённости учётных записей в социальных сетях требует не только развития технологий безопасности со стороны платформ, но и системного повышения цифровой грамотности самих пользователей.

_____

* Facebook — социальная сеть, принадлежащая компании Meta** Platforms, Inc.

** Meta — деятельность Meta признана экстремистской и запрещена на территории Российской Федерации.

*** X (до 2023 года — Twitter) — социальная сеть, заблокированная на территории Российской Федерации.

Использованная литература

1. Securitylab.ru. Свыше 100 млн пользователей «ВКонтакте» стали жертвами масштабного взлома. - 2016. - URL: https://www.securitylab.ru/news/482643.php (дата обращения: 06.07.2026).

2. РБК. Эксперты обнаружили утечку данных полумиллиарда пользователей Facebook* - 2021. - URL: https://www.rbc.ru/technology_and_media/03/04/2021/60688ff99a7947cac2a65f28 (дата обращения: 07.07.2026).

3. Hi-Tech Mail. Мегаслив: в сеть попало 26 миллиардов данных пользователей с площадок X***, ВК, Telegram и других. - 2024. - URL: https://hi-tech.mail.ru/news/105888 (дата обращения: 07.07.2026).
4. TAdviser. Утечки данных в России. - 2025–2026. - URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_России (дата обращения: 07.07.2026).
5. Хакер (xakep.ru). Microsoft: только 11% корпоративных аккаунтов используют мультифакторную аутентификацию. - 2020. - URL: https://xakep.ru/2020/03/06/microsoft-mfa-stats/ (дата обращения: 07.07.2026).
6. Инфратех (корпоративный блог). Многофакторная аутентификация MFA — выбор и внедрение решений для безопасности. - 2025. - URL: https://blog.infra-tech.ru/mfa-dlya-biznesa/ (дата обращения: 07.07.2026).
7. Контур.Эгида. Двухфакторная аутентификация: плюсы и минусы основных способов. - 2025. - URL: https://kontur.ru/aegis/blog/55728-dvuhfaktornaya_autentifikaciya (дата обращения: 07.07.2026).
8. Multifactor. Двухфакторная аутентификация (2FA): что это, как работает и для чего она нужна. - 2025. - URL: https://multifactor.ru/press-center/dvuhfaktornaya-autentifikacziya-chto-eto-takoe-i-zachem-ona-nuzhna/ (дата обращения: 07.07.2026).
9. Habr.com. Данные более 100 млн аккаунтов «Вконтакте» продаются в сети за 1 биткоин. - 2016. - URL: https://habr.com/ru/articles/394973/ (дата обращения: 07.07.2026).
10. Forbes.ru. Личные данные и номера 500 млн пользователей Facebook* попали в сеть. - 2021. - URL: https://www.forbes.ru/newsroom/tehnologii/425327 (дата обращения: 07.07.2026).
11. Российская газета. «Длина» новой утечки данных из Telegram, VK и других сервисов составила 16 тысяч км. - 2024. - URL: https://rg.ru/2024/01/26/ (дата обращения: 07.07.2026).

12. Инфратех. Подозрительная активность: что делать, если аккаунт заблокирован, и как распознать взлом. - 2026. - URL: https://blog.infra-tech.ru/podozritelnaya-aktivnost/ (дата обращения: 07.07.2026).
13. Kaspersky Daily. Что такое credential stuffing и чем он опасен. - URL: https://www.kaspersky.ru/blog/what-is-credential-stuffing/37385/ (дата обращения: 07.07.2026).
14. Kaspersky Daily. Что такое SIM-свопинг и как от него защититься. - URL: https://www.kaspersky.ru/blog/what-is-sim-swapping/37134/ (дата обращения: 07.07.2026).
15. Пронкина Е.С. Парадокс приватности: почему пользователи социальных медиа раскрывают персональную информацию в публичном пространстве // Вестник РГГУ. Серия «Философия. Социология. Искусствоведение». 2018. № 8-1. С. 155 - 165.

Used literature

1. Securitylab.ru. Over 100 million VKontakte users have become victims of a large-scale hack. - 2016. - URL: https://www.securitylab.ru/news/482643.php (date of access: 07/06/2026).
2. RBC. Experts have discovered a data leak of half a billion Facebook users* - 2021. - URL: https://www.rbc.ru/technology_and_media/03/04/2021/60688ff99a7947cac2a65f28 (date of request: 07.07.2026).
3. Hi-Tech Mail. Mega-spill: 26 billion user data from X***, VK, Telegram and others platforms got into the network. - 2024. - URL: https://hi-tech.mail.ru/news/105888 (date of request: 07/07/2026).
4. TAdviser. Data leaks in Russia. - 2025-2026. - URL: https://www.tadviser.ru/index.php/Статья:Data leaks_in_Russia (date of access: 07.07.2026).
5. Hacker (xakep.ru). Microsoft: Only 11% of corporate accounts use multifactor authentication. - 2020. - URL: https://xakep.ru/2020/03/06/microsoft-mfa-stats / (date of access: 07.07.2026).

6. Infratech (corporate blog). Multi-factor authentication MFA — selection and implementation of security solutions. - 2025. - URL: https://blog.infra-tech.ru/mfa-dlya-biznesa / (date of access: 07.07.2026).
7. Contour.Aegis. Two-factor authentication: the pros and cons of the main methods. - 2025. - URL: https://kontur.ru/aegis/blog/55728-dvuhfaktornaya_autentifikaciya (date of request: 07.07.2026).
8. Multifactor. Two-factor authentication (2FA): what it is, how it works, and what it's for. - 2025. - URL: https://multifactor.ru/press-center/dvuhfaktornaya-autentifikacziya-chto-eto-takoe-i-zachem-ona-nuzhna / (date of access: 07.07.2026).
9. Habr.com . The data of more than 100 million Vkontakte accounts are sold online for 1 bitcoin. - 2016. - URL: https://habr.com/ru/articles/394973 / (date of access: 07.07.2026).
10. Forbes.ru Personal data and numbers of 500 million Facebook users* have been uploaded to the network. - 2021. - URL: https://www.forbes.ru/newsroom/tehnologii/425327 (date of request: 07.07.2026).
11. Rossiyskaya gazeta. The "length" of the new data leak from Telegram, VK and other services was 16 thousand km. - 2024. - URL: https://rg.ru/2024/01/26 / (date of access: 07.07.2026).
12. Infratech. Suspicious activity: what to do if your account is blocked, and how to detect a hack. - 2026. - URL: https://blog.infra-tech.ru/podozritelnaya-aktivnost / (date of access: 07.07.2026).
13. Kaspersky Daily. What is credential stuffing and how it is dangerous. - URL: https://www.kaspersky.ru/blog/what-is-credential-stuffing/37385 / (date of access: 07.07.2026).
14. Kaspersky Daily. What is SIM swapping and how to protect yourself from it. - URL: https://www.kaspersky.ru/blog/what-is-sim-swapping/37134 / (date of access: 07.07.2026).
15. Pronkina E.S. The paradox of privacy: why users of social media disclose personal information in the public space // Bulletin of the Russian State University

of Economics. The series "Philosophy. Sociology. Art history". 2018. No. 8-1. pp. 155 - 165.