БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 4 (119). – 59–74

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-4-59-74

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ КИБЕРМОШЕННИЧЕСТВЕ ЗА СЧЕТ ПОВЫШЕНИЯ ЭМОЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ПОЛЬЗОВАТЕЛЕЙ*

Л.А. ЛАРИОНОВА[1], Ю.В. СИБИРЯК[2]

[1] *РФ, 664074, г. Иркутск, ул. Лермонтова, 83, Иркутский национальный исследовательский технический университет, доцент Центра компетенций по кибербезопасности. E-mail: lal44@mail.ru*
[2] *РФ, 630102, г. Новосибирск, ул. Кирова, 86, Сибирский государственный университет телекоммуникаций и информатики, и. о. директора Института информационной безопасности. E-mail: yury.sibiryak@yandex.ru*

Современное кибермошенничество приобретает все более изощренные формы, позволяя злоумышленникам использовать не только технические уязвимости, но и особенности человеческой психики. В центре внимания статьи чувствительные данные пользователей и их эмоциональная уязвимость, которые в совокупности образуют критическую точку риска при атаке. Ключевой проблемой становится многогранное воздействие, при котором эмоциональное давление усиливает результативность технических атак, а технические сбои усугубляют психологическое состояние пользователей, создавая замкнутый цикл уязвимости. В работе рассмотрена интеграция комплексной системы безопасности – технических и психологических аспектов.

Ключевые слова: чувствительные данные, эмоциональная уязвимость, социальная инженерия, кибермошенничество, комплексная система безопасности

ВВЕДЕНИЕ

Углубленный анализ чувствительных данных и эмоциональной уязвимости пользователя в контексте кибермошенничества обусловлен растущей сложностью и масштабами киберпреступлений в 2025 году, когда искусственный интеллект и машинное обучение активно использовались злоумышленниками для проведения целенаправленных атак, включая социальную ин-

* Статья получена 11 ноября 2025 г.

женерию. Это требует применения передовых методов анализа больших данных и технологий предсказательного анализа угроз для своевременного выявления уязвимостей и защиты чувствительной информации. Кроме того, эмоциональная уязвимость пользователя становится ключевым фактором успешности мошеннических схем, что делает необходимым интеграцию психологических аспектов в системы информационной безопасности для повышения эффективности защиты и формирования устойчивости пользователей к киберугрозам [1].

В современных системах защиты данные анонимизируются и шифруются. Это повышает требования к анализу и мониторингу поведения пользователей для выявления аномалий, связанных с попытками мошенничества и утечек. Также важно учитывать использование AI-ассистентов и аналитики поведения для быстрого реагирования на инциденты и минимизации ущерба.

Таким образом, углубленный анализ чувствительных данных в сочетании с пониманием эмоциональной составляющей пользователей способствует развитию комплексных подходов к противодействию кибермошенничеству, что актуально в условиях постоянного эволюционирования киберугроз и технологических изменений в 2025 году.

В центре внимания статьи чувствительные данные пользователей и их эмоциональная уязвимость, которые в совокупности образуют критическую точку риска при атаке.

1. ОПИСАНИЕ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ И ЭМОЦИОНАЛЬНОЙ УЯЗВИМОСТИ

Чувствительные данные – это сведения, позволяющие идентифицировать личность, получить доступ к финансовым и иным важным ресурсам. Их защита осложняется широкой распространенностью цифровых коммуникаций и регулярной передачей информации через разнообразные платформы. Злоумышленники активно эксплуатируют психологические характеристики человека, такие как желание помочь, страх потерять выгоду или получить уникальное предложение, что значительно повышает вероятность успешной атаки. Эта взаимосвязь между психологическими и техническими аспектами создает сложную систему угроз, требующую комплексных мер исследования и нейтрализации.

Схема чувствительных данных представлена на рис. 1.

Для глубокого понимания природы подобных угроз необходимо рассмотреть психологические основы эмоциональной уязвимости. Эмоции могут влиять на восприятие информации и способность критически оценивать получаемые сообщения. Сильные эмоциональные состояния, например тревога или

радость, снижают уровень рационального мышления, что делает пользователя более восприимчивым к манипуляциям [3].

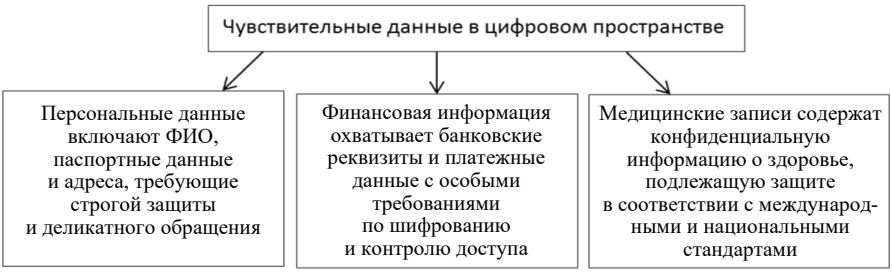

Рис. 1. Схема чувствительных данных

Эмоциональная уязвимость в онлайн-среде определяется как состояние повышенной восприимчивости пользователя к психологическим воздействиям, обусловленное изменением эмоционального фона и снижением критического восприятия информации. Она проявляется в усилении ощущений тревоги, страха, неуверенности и стресса, которые ослабляют способность к рациональному анализу происходящего и принятию взвешенных решений. Такая уязвимость создает благоприятные условия для манипуляций, поскольку эмоциональное напряжение снижает контроль личности над своим поведением и когнитивными процессами [6].

Одним из фундаментальных механизмов влияния является страх – реакция, связанная с угрозой потери или опасностью, которая активирует у человека инстинкты самосохранения. В цифровом пространстве страх может возникать на фоне угроз безопасности персональных данных, финансовых потерь или социального осуждения. Тревога, в свою очередь, формирует затуманенное восприятие ситуации, что вызывает ошибочные оценки и подверженность внешним внушениям. Это состояние снижает способность фильтровать и критически оценивать получаемую информацию, делая пользователя легкой мишенью для мошеннических схем. Доверие, базирующееся на предположении о доброжелательности источника информации, играет ключевую роль: именно оно часто используется злоумышленниками для установления эмоционального контакта и манипулирования жертвой [6].

Когнитивные искажения, возникающие под воздействием эмоционального напряжения, усиливают уязвимость. Таким искажением является, например, эффект подтверждения, когда человек склонен воспринимать лишь ту информацию, которая согласуется с его ожиданиями, и игнорировать контраргументы. Эффект доверия, при котором человек переоценивает досто-

верность сообщения из-за симпатии, также способствует созданию ложного ощущения безопасности. Импульсивность, вызванная эмоциональным возбуждением, ведет к принятию поспешных решений без должной проверки фактов (рис. 2). В совокупности эти механизмы усиливают риски стать жертвой кибермошенничества, так как снижают уровень критического мышления и повышают склонность к необдуманным действиям [4].

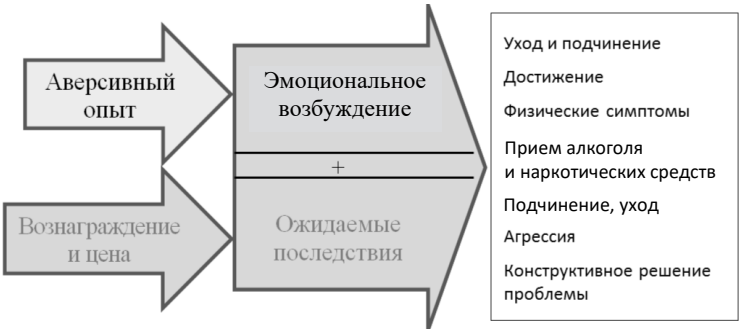

Рис. 2. Влияние зависимости на активность пользователя

Особое значение в развитии эмоциональной уязвимости имеют социальные сети, которые с помощью сложных алгоритмов выявляют эмоциональные состояния пользователей – моменты сомнений, тревожности или заниженной самооценки. Эти данные используются для таргетинга рекламы и контента, вызывающего резонанс с текущим эмоциональным фоном. Например, если пользователь удаляет селфи, система зачастую оперативно предлагает косметические средства, что отражает эксплуатацию внутренней неуверенности. Манипуляции усиливаются у уязвимых групп (подростков, молодых мам и др.), которым сложнее удерживать психологический баланс в виртуальном пространстве. Например, информация о гормональных циклах женщин применяется для точного таргетинга в периоды, когда склонность к импульсивным покупкам возрастает, что свидетельствует о глубокой аналитике эмоциональных факторов [2].

Такое использование эмоциональной уязвимости вызывает опасения, поскольку ведет к цифровой эксплуатации, истощению ресурсов психики и формированию психологической зависимости от внешних стимулов. Пользователи, испытывающие стресс и давление окружающей онлайн-среды, зачастую не осознают масштаб своей подверженности эмоциональному воздействию, что усиливает возможность психологических манипуляций и социального отчуждения [8]. Устойчивость к таким воздействиям требует осознанно-

сти и формирования личных стратегий психологической защиты, направленных на сохранение внутренней гармонии и критического восприятия цифрового контента.

Важной концепцией для понимания эмоциональной уязвимости является идея, предполагающая принятие своей уязвимости как части естественного взаимодействия с цифровым миром. Это предполагает не пассивность, а активное стремление к гармонизации и адаптации, что способствует снижению риска потери контроля и необдуманных решений под влиянием негативных эмоций.

Таким образом, понимание психологических факторов является ключом к выявлению эффективных методов противодействия социальной инженерии [9].

Схема чувствительных данных пользователей и их эмоциональная уязвимость как совокупность критической точки риска при атаке представлена на рис. 3.

Рис. 3. Схема чувствительных данных пользователей и их эмоциональная уязвимость как совокупность критической точки риска при атаках

2. ПСИХОЛОГИЧЕСКИЕ ОСНОВЫ ЭМОЦИОНАЛЬНОЙ УЯЗВИМОСТИ В КИБЕРПРОСТРАНСТВЕ

В современных условиях усиления киберугроз изучение методов социальной инженерии приобретает критическое значение для понимания и предотвращения мошеннических действий.

Этот подход основан на эксплуатации эмоций пользователей и их психологических особенностей для получения конфиденциальной информации без прямого технического взлома. Рост числа зарегистрированных IT-преступлений и значительные финансовые потери свидетельствуют о высокой эффективности таких методов и необходимости системного анализа существующих приёмов манипуляций [10].

Основные механизмы социального воздействия строятся на трех ключевых эмоциональных триггерах: страхе, доверии и срочности. Страх инициирует автоматическую реакцию на угрозу, заставляя жертву принимать решения под давлением, часто без должной проверки обстоятельств. Мошенники часто представляются сотрудниками банков или государственных структур, сообщая о компрометации учетной записи или подозрительной активности и требуя немедленных действий. Этот прием вызывает панику и снижает критичность мышления, что способствует раскрытию паролей, кодов из СМС и другой чувствительной информации [11].

Доверие используется в качестве инструмента установления эмоционального контакта. Злоумышленники тщательно готовятся: собирают данные о жертве, создавая убедительную предысторию – претекстинг (например, обращаются от имени известных организаций или коллег). В результате жертва воспринимает собеседника как надежного партнера, что снижает барьеры недоверия и стимулирует раскрытие закрытой информации. Часто подобные атаки развиваются поэтапно: сначала осуществляется исследование и налаживание контакта, затем извлечение нужных данных посредством личного убеждения или просьб о помощи (обратная социальная инженерия) [7].

Срочность является мощным драйвером немедленного реагирования без анализа рисков. Создание искусственного дефицита времени («Ваш аккаунт будет заблокирован через 10 минут», «Акция действует только сегодня») заставляет пользователя игнорировать стандартные меры предосторожности. В атаках типа фишинга используется этот прием, т. е. отправляются поддельные письма или SMS с требованием срочных действий: перейти по ссылке, обновить данные или подтвердить личность. Из-за давления на психику жертва может совершить необдуманный шаг (например, ввести банковские реквизиты на мошенническом сайте или установить вредоносное ПО под видом обновления).

Телефонные звонки (вишинг) играют особую роль в манипуляциях эмоциями, так как голос и интонация усиливают эффект сопереживания и доверия. Злоумышленники имитируют официальный тон и демонстрируют знание личных деталей, что дает ощущение легитимности. Это снижает бдительность и стимулирует жертву к непосредственному взаимодействию, часто с раскрытием конфиденциальной информации или запуском вредоносных программ.

Физические методы, такие как «дорожное яблоко» – распространение зараженных флеш-накопителей, создают дополнительный вектор угрозы, используя привычку доверять файлам или устройствам, обнаруженным в офисе или на улице. Этот способ действует на эмоциональном уровне невнимательности и любознательности с последующим техническим заражением системы [7].

Таким образом, социальная инженерия представляет собой комплекс приемов, направленных на сознательное использование эмоциональной уязвимости жертв. Мошенники искусно комбинируют страх, доверие и срочность для максимального снижения критического восприятия и ускорения принятия решений, приводящих к компрометации данных. Повышение осведомленности о таких методах существенно снижает вероятность успешного мошенничества.

3. КЛИЕНТСКИЕ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИХ РОЛЬ В КОМПРОМЕТАЦИИ ДАННЫХ

Клиентские уязвимости представляют собой технические дефекты или ошибки в программном обеспечении, которые могут быть использованы злоумышленниками для обхода средств защиты и получения несанкционированного доступа к данным пользователя. В частности, уязвимости веб-браузеров и мобильных приложений выступают критическим каналом компрометации чувствительной информации, поскольку они непосредственно взаимодействуют с пользователем и операционной системой устройства.

Мобильные приложения имеют ряд особенностей, отличающих их от традиционных веб-приложений. Они интегрируются с системными компонентами устройства, что предоставляет потенциальному атакующему расширенные возможности, включая доступ к системным вызовам, файловой системе и аппаратным ресурсам. Согласно исследованию Positive Technologies, 76 % мобильных приложений содержат уязвимости высокого уровня риска, а 43 % – критические уязвимости, которые могут быть использованы для получения конфиденциальных данных или контроля над устройством. За 2024 год было зафиксировано свыше 2,3 миллиарда утечек персональных данных, инициированных через мобильные приложения, что подчеркивает масштаб угрозы.

Ключевыми категориями уязвимостей являются ошибки в аутентификации и авторизации, составляющие примерно треть всех выявленных проблем. Они позволяют злоумышленникам получить несанкционированный доступ к аккаунтам и функциям приложения. Другой значимой проблемой можно назвать возможность повышения привилегий – получение root-доступа на Android или jailbreak на iOS, способствующего обходу системных ограничений и внедрению вредоносного кода.

Частые ошибки в реализации протоколов SSL/TLS и использовании устаревших библиотек, таких как OpenSSL и AFNetworking, способствуют возникновению атак «человек посередине» (MITM). Некорректное отключение механизмов проверки сертификатов снижает безопасность сетевого взаимодействия, позволяя перехватывать и изменять передаваемые данные. Помимо этого, популярные уязвимости включают XSS (межсайтовый скриптинг), SQL-инъекции и XXE-атаки, которые особенно опасны в мобильных банковских приложениях. Так, 35 % приложений на iOS и 15 % на Android подвержены SSL-проблемам, 22 % iOS-приложений – SQL-инъекциям, а 70 % iOS и 20 % Android – XSS-уязвимостям [9].

Уязвимости касаются и межпроцессного взаимодействия: 22 % Android-приложений используют его некорректно, что позволяет сторонним приложениям получать доступ к банковской информации. Эти нарушения безопасности нередко становятся причиной финансовых потерь пользователей и ущерба для компаний.

Для снижения рисков реализации уязвимостей рекомендуется использование различных технических методов защиты, включая обфускацию исходного кода, шифрование критичных данных, внедрение песочниц (sandbox), корректное управление разрешениями и применение комплексных мер сетевой безопасности. Важную роль играет непрерывный мониторинг безопасности и регулярное обновление программного обеспечения, что позволяет своевременно устранять выявленные проблемы и затруднять действия злоумышленников [13].

Отдельной проблемой является замедленная реакция конечных пользователей на обновления приложений и невозможность автоматической замены уязвимых библиотек операционными системами, что продлевает срок эксплуатации уязвимого кода и увеличивает шанс успешной атаки. В совокупности эти факторы делают клиентские уязвимости существенной технической угрозой и основой для дальнейших кибератак [13].

Отсутствие своевременного обновления программного обеспечения значительно увеличивает риск эксплуатации этих уязвимостей.

4. КОМПЛЕКСНЫЙ ВЗГЛЯД НА КИБЕРУГРОЗЫ И МЕТОДЫ ПОВЫШЕНИЯ ЭМОЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ПОЛЬЗОВАТЕЛЕЙ

Междисциплинарный подход к анализу информационной безопасности становится необходимостью в условиях растущей сложности киберугроз. Эффективное противодействие современным атакам требует не отдельного

рассмотрения технических уязвимостей или психологических особенностей пользователей, а их интеграции для создания целостной картины воздействия на защищенность информационных ресурсов [5]. Эмоциональная уязвимость пользователя усиливает опасность технических дефектов программного обеспечения и сетевых протоколов, превращая потенциально нейтральные уязвимости в активные точки проникновения злоумышленников.

Психологический фактор влияет на поведение пользователя в ситуациях повышенного риска, снижая эффективность встроенных технических механизмов защиты. Например, спровоцированное страхом или давлением чувства срочности могут заставить жертву проигнорировать предупреждения системы о подозрительной активности или установить вредоносное ПО под видом обновления, тем самым открывая дверь для эксплуатации клиентских уязвимостей. В этом контексте даже сложные криптографические методы и многоуровневая аутентификация могут оказаться недостаточными, если пользователь отказывается соблюдать базовые правила кибергигиены или не в состоянии это делать.

Обратное взаимодействие также имеет место: технические риски усугубляют эмоциональное состояние пользователей. Частые и повторяющиеся инциденты, такие как утечки данных или фишинговые атаки, ведут к повышению тревожности, потере доверия и развитию когнитивных искажений, которые увеличивают вероятность повторной компрометации. Условия постоянного давления создают почву для манипуляций через социальную инженерию, формируя замкнутый круг взаимного усиления технических и психологических угроз.

Непрерывное развитие атакующих методов приводит к созданию многоступенчатых стратегий, в которых эмоциональное воздействие и технические уязвимости выступают взаимодополняющими инструментами. Так, социальные инженерные приемы получают усиление через использование программных багов для автоматического сбора данных или обхода защитных механизмов. Это позволяет злоумышленникам проводить целенаправленное воздействие на конкретных пользователей с повышенной вероятностью успеха, учитывая их индивидуальные эмоциональные особенности и имеющиеся технические слабости.

В связи с изложенным становится очевидной необходимость комплексной системы безопасности, которая одновременно решает задачи технической защиты и формирования устойчивой психологической позиции пользователей. Организационные меры, включая обучение и тренинги по распознаванию фишинга и социальной инженерии, интегрированные с использованием современных средств мониторинга и предотвращения утечек данных, снижают общую уязвимость информационной среды. Такой подход уменьшает влияние

человеческого фактора, минимизирует возможности для эксплуатации технических пробелов и повышает адаптивность системы к новым видам угроз.

Анализ жизненного цикла кибератак и способов интеграции эмоциональных и технических факторов позволяет выявить уязвимые точки на каждом этапе – от рекогносцировки до реализации вредоносных действий. Своевременное выявление признаков эмоционального давления и технических аномалий дает возможность применять меры превентивного характера и снижать последствия инцидентов. В комплексе с цифровизацией экономики и ростом киберрисков это становится необходимым элементом обеспечения национальных интересов и устойчивого функционирования бизнеса [5].

Комплексный анализ таких угроз критичен для разработки эффективных мер защиты.

Эмоциональный аспект играет ключевую роль в обеспечении безопасности пользователя в цифровом пространстве, поскольку именно состояние психики влияет на восприятие информации и способность противостоять манипуляциям. Улучшение эмоциональной устойчивости позволяет снизить воздействие стрессовых факторов, интегрированных в кибермошенничество, и усиливает способность рационально оценивать угрозы без излишней паники или импульсивных реакций.

Важным направлением является развитие навыков критического мышления и умения распознавать манипуляции. Обучение должно включать понимание типичных эмоциональных триггеров – страха, срочности, любопытства, которые используют мошенники, и формирование стратегии осознанного реагирования на них. Пользователи, обладающие умением отделять факты от эмоций и задавать вопросы по поводу источника и содержания информации, существенно снижают вероятность попадания в ловушку социальной инженерии [12].

Формирование эмоциональных границ в интернет-среде – еще одна важная стратегия. Это включает осознание собственного эмоционального состояния и умение контролировать свои реакции на негативный или провокационный контент. Способность воспринимать информацию дистанцированно и сохранять чувство самоуважения помогает предотвращать распространение стрессовых состояний и укреплять психическую стабильность. Рекомендуется сознательно ограничивать раскрытие личных данных и делиться в интернете лишь тем, что действительно хочется показать, избегая излишней экспозиции и, как следствие, снижения уязвимости [12].

Таким образом, целенаправленное повышение эмоциональной устойчивости включает системное обучение критическому восприятию информации, развитие навыков саморегуляции и умение создавать здоровые эмоциональные границы при взаимодействии с цифровым контентом. Обеспечение

таких психологических ресурсов наряду с техническими мерами создает прочный фундамент для защиты личности в условиях эволюции киберугроз. Эмоциональная устойчивость снижает вероятность успешного воздействия мошенников.

Комплексная система безопасности: технические и психологические аспекты

Компонент	Описание мер	Преимущества
Организационные меры	Обучение и тренинги по распознаванию фишинга, социальной инженерии; мониторинг и предотвращение утечек данных	Снижение влияния человеческого фактора, минимизация эксплуатации технических пробелов, повышение адаптивности к угрозам
Анализ жизненного цикла кибератак	Выявление уязвимых точек (рекогносцировка до реализации); интеграция эмоциональных и технических факторов	Превентивные меры, снижение последствий инцидентов, защита национальных интересов и бизнеса в условиях цифровизации
Эмоциональная устойчивость	Улучшение психики для противостояния манипуляциям; развитие критического мышления против триггеров (страх, срочность)	Рациональная оценка угроз, снижение воздействия стресса в кибермошенничестве
Формирование эмоциональных границ	Осознание состояния, контроль реакций; ограничение раскрытия личных данных в сети	Предотвращение стресса, укрепление психической стабильности, дистанцированное восприятие контента

ЗАКЛЮЧЕНИЕ

Рассмотренные механизмы социальной инженерии демонстрируют, как злоумышленники используют эмоции страха, доверия и срочности для манипулирования, снижая бдительность и рациональное восприятие информации. Анализ когнитивных искажений подтверждает, что под воздействием эмоционального давления пользователи склонны принимать решения, противоречащие собственным интересам и безопасности. Одновременно клиентские уязвимости программного обеспечения открывают доступ по техническим

каналам, позволяя злоумышленникам активно их использовать в мошеннических схемах.

Проведенный комплексный анализ взаимодействия эмоциональной уязвимости и технических рисков подчеркивает необходимость системного подхода к обеспечению безопасности. Отдельное повышение устойчивости пользователя к эмоциональным воздействиям оказывается неэффективным без одновременного усиления технических барьеров. Поэтому сочетание методов психологической защиты, таких как развитие критического мышления, обучение цифровой грамотности и формирование здоровых эмоциональных границ, с современными техническими средствами – от шифрования до систем мониторинга – создает надежный фундамент для минимизации рисков.

Внедрение комплексных стратегий защиты обусловливает необходимость регулярного обновления знаний и технологий, а также активного вовлечения самих пользователей в процесс безопасности. Особое внимание следует уделить развитию обучающих программ, способствующих повышению цифровой компетенции, осознанному отношению к рискам и, как следствие, снижению вероятности успешных атак посредством социальной инженерии. Одновременно технические решения должны адаптироваться к быстрому развитию угроз, обеспечивая устойчивость информационных систем.

Итак, противостояние современному кибермошенничеству требует синергии психологических и технических мер. Предложенные подходы и рекомендации представляют собой эффективный инструментарий для специалистов в области информационной безопасности и юридической психологии и для всех пользователей, стремящихся повысить уровень своей защиты в киберпространстве. Только комплексное понимание проблемы и системная реализация предложенных методов позволяет значительно снизить уязвимость и обеспечить долгосрочную безопасность чувствительных данных и эмоционального состояния в условиях быстро меняющегося цифрового мира.

СПИСОК ЛИТЕРАТУРЫ

1. *Азбиева У.Р., Мамаева А.А., Кувшинова Ю.А.* Цифровая грамотность и кибермошенничество: новые вызовы для российской экономики знаний // Вестник Национального института бизнеса. – 2025. – № 2 (58). – С. 341–350.

2. *Андреев И.В.* Формирование психологической устойчивости студентов к негативному влиянию интернет-технологий: дис. ... канд. психол. наук: 19.00.07. – Н. Новгород, 2008. – 215 с.

3. *Быковская Е.Д.* Психологический портрет пользователя социальной сети с выраженным полюсом личного конструкта «эмоциональная устойчивость – эмоциональная неустойчивость» // Научные стремления. – 2016. – Вып. 20. – С. 117–119.

4. *Викторова Е.В., Бадаева Е.Р.* Культурно-психологический анализ влияния эмоциогенных свойств цифрового контента на пользователей подростково-юношеского возраста // Коммуникология. – 2020. – Т. 8, № 3. – С. 126–137.

5. *Вострецова Е.В.* Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.

6. Психологическая уязвимость: риск молодежного взаимодействия в сети Интернет: монография / Ю.Р. Тагильцева, М.Р. Бабикова, И.В. Воробьева, О.В. Кружкова, Д.В. Руденкин. – Екатеринбург: Урал. гос. пед. ун-т, 2020. – 160 с.

7. *Янгаева М.О.* Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. – 2021. – № 1 (42). – С. 133–138.

8. *Зотина Е.В.* Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. – 2022. – Т. 13, № 4 (50). – С. 93–99.

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

10. *Михалёва У.А.* Претекстинг и способы противодействия ему // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – № 50 (2). – С. 109–116. – DOI: 10.21822/2073-6185-2023-50-2-109-116.

11. Методика защиты организации от атак с использованием социальной инженерии механизмами автоматизированных программ / О.М. Штеренберг, В.И. Андрианов, А.Ю. Хоромская, В.В. Максимов, В.В. Сигачева // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1, Естественные и технические науки. – 2023. – № 3. – С. 120–127. – DOI: 10.46418/2079-8199-2023-3-19.

12. *Штеренберг С.И., Данилова Ю.С.* Разработка методики внедрения и выявления эффективности siem-системы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1, Естественные и технические науки. – 2020. – № 3. – С. 40–45. – DOI: 10.46418/2079-8199_2020_3_6.

13. Формализация подхода к определению актуальности угроз информационной безопасности / О.М. Голембиовская, М.Ю. Рытов, М.М. Голембиовский [и др.]. – Саратов: Вузовское образование, 2022. – 147 с. – ISBN 978-5-4487-0840-4.

Ларионова Лариса Александровна, доцент Центра компетенций по кибербезопасности Иркутского национального исследовательского технического университета. Основное направление научных исследований – социальная инженерия. E-mail: lal44@mail.ru

Сибиряк Юрий Владимирович, и. о. директора Института информационной безопасности Сибирского государственного университета телекоммуникаций и информатики. Основное направление научных исследований – система менеджмента информационной безопасности. E-mail: yury.sibiryak@yandex.ru

DOI: 10.17212/2782-2230-2025-4-59-74

Ensuring information security against cyber fraud by increasing the emotional resilience of users*

L.A. Larionova[1], Yu.V. Sibiryak[2]

[1] *IRNTU, 83 Lermontov Street, Irkutsk, 664074, Russian Federation, Associate Professor at the Cybersecurity Competence Center. E-mail: lal44@mail.ru*
[2] *SibSUTIS, 86 Kirov Street, Novosibirsk, 630102, Russian Federation, Acting Director of the Institute of Information Security. E-mail: yury.sibiryak@yandex.ru*

Modern cyberbullying is becoming more and more sophisticated, allowing attackers to exploit not only technical vulnerabilities, but also the peculiarities of the human psyche. The focus of this work is on the sensitive data of users and their emotional vulnerability, which together form a critical point of risk during an attack. The key problem is the multifaceted impact, in which emotional pressure increases the effectiveness of technical attacks, and technical failures worsen the psychological state of users, creating a vicious cycle of vulnerability. The paper considers sensitive data and emotional vulnerabilities of users, as well as the integration of a comprehensive security system: technical and psychological aspects.

Keywords: sensitive data, emotional vulnerability, social engineering, cyberbullying, integrated security system

* *Received 11 November 2025.*

REFERENCES

1. Azbieva U.R., Mamaeva A.A., Kuvshinova Yu.A. Tsifrovaya gramotnost' i kiber-moshennichestvo: novye vyzovy dlya rossiiskoi ekonomiki znanii [Digital literacy and cyberbullying: new challenges for the russian knowledge economy]. *Vestnik Natsional'nogo instituta biznesa*, 2025, no. 2 (58), pp. 341–350. (In Russian).

2. Andreev I.V. *Formirovanie psikhologicheskoi ustoichivosti studentov k negativnomu vliyaniyu internet-tekhnologii*. Diss. kand. psikhol. nauk [The formation of psychological stability of students to the negative impact of Internet technologies. PhD Psychological sci. diss.]. Nizhny Novgorod, 2008. 215 p.

3. Bykovskaya E.D. Psikhologicheskii portret pol'zovatelya sotsial'noi seti s vyrazhennym polyusom lichnogo konstrukta «emotsional'naya ustoichivost' – emotsional'naya neustoichivost'» [Psychological portrait users of social internet with pronounced poles personal constructs "emotional stability – emotional instability"]. *Nauchnye stremleniya = Scientific Aspirations*, 2016, iss. 20, pp. 117–119.

4. Viktorova E.V., Badaeva E.R. Kul'turno-psikhologicheskii analiz vliyaniya emo-tsiogennykh svoistv tsifrovogo kontenta na pol'zovatelei podrostkovo-yunosheskogo vozrasta [Cultural-psychological analysis of the influence of emotiogenic properties of digital content on adolescent users]. *Kommunikologiya = Communicology*, 2020, vol. 8, no. 3, pp. 126–137.

5. Vostretsova E.V. *Osnovy informatsionnoi bezopasnosti* [Fundamentals of information security]. Yekaterinburg, Ural University Publ, 2019. 204 p.

6. Tagil'tseva Yu.R., Babikova M.R., Vorob'eva I.V., Kruzhkova O.V., Rudenkin D.V. *Psikhologicheskaya uyazvimost': risk molodezhnogo vzaimodeistviya v seti Internet* [Psychological vulnerability: risk of youth interaction on the Internet]. Yekaterinburg, Ural State Pedagogical University Publ., 2020. 160 p.

7. Yangaeva M.O. Sotsial'naya inzheneriya kak sposob sovershеniya kiberprestuplenii [Social engineering as a way to committing cyber crimes]. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii = Vestnik of Siberian law institute of the MIA of Russia*, 2021, no. 1 (42), pp. 133–138.

8. Zotina E.V. Pretekstinq kak priem sotsial'noi inzhenerii, ispol'zuemyi telefonnymi moshennikami: kriminologicheskii vzglyad na problemu [Pretexting as a social engineering technique used by telephone scammers: a criminological view of the problem]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2022, vol. 13, no. 4 (50), pp. 93–99.

9. Markelov V.K., Privalov A.N. Metod pretekstinga kak ugroza informatsionnoi bezopasnosti v sotsial'nykh setyakh [Pretexting method as a threat to information security in social networks]. *Vestnik Adygeiskogo gosudarstvennogo univer-*

siteta. Seriya: Estestvenno-matematicheskie i tekhnicheskie nauki = Bulletin of the Adygea State University. Series: Natural-mathematical and technical sciences, 2024, no. 2 (341), pp. 51–61. DOI: 10.53598/2410-3225-2024-2-341-51-61.

10. Mikhaleva U.A. Preteksting i sposoby protivodeistviya emu [Pretexting and means to counter it]. *Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki = Herald of Dagestan State Technical University. Technical Sciences*, 2023, no. 50 (2), pp. 109–116. DOI: 10.21822/2073-6185-2023-50-2-109-116.

11. Shterenberg O.M., Andrianov V.I., Khoromskaya A.Yu., Maksimov V.V., Sigacheva V.V. Metodika zashchity organizatsii ot atak s ispol'zovaniem sotsial'noi inzhenerii mekhanizmami avtomatizirovannykh programm [Ways to protect an organization from attacks using social engineering]. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizaina. Seriya 1, Estestvennye i tekhnicheskie nauki = Vestnik of St. Petersburg state university of technology and design. Series 1, Natural and technical sciences*, 2023, no. 3, pp. 120–127. DOI: 10.46418/2079-8199-2023-3-19.

12. Shterenberg S.I., Danilova Yu.S. Razrabotka metodiki vnedreniya i vyyavleniya effektivnosti siem-sistemy [Implementation methodology and calculation of the efficiency of a siem-system]. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizaina. Seriya 1, Estestvennye i tekhnicheskie nauki = Vestnik of St. Petersburg state university of technology and design. Series 1, Natural and technical sciences*, 2020, no. 3, pp. 40–45. DOI: 10.46418/2079-8199_2020_3_6.

13. Golembiovskaya O.M., Rytov M.Yu., Golembiovskii M.M., Shinakov K.E., Bannikov A.I., Kondrashova E.V., Doroshenko V.Yu. *Formalizatsiya podkhoda k opredeleniyu aktual'nosti ugroz informatsionnoi bezopasnosti* [Formalization of the approach to determining the relevance of information security threats]. Saratov, Vuzovskoe obrazovanie Publ., 2022. 147 p. ISBN 978-5-4487-0840-4.

Для цитирования:

Ларионова Л.А., Сибиряк Ю.В. Обеспечение информационной безопасности при кибермошенничестве за счет повышения эмоциональной устойчивости пользователей // Безопасность цифровых технологий. – 2025. – № 4 (119). – С. 59–74. – DOI: 10.17212/2782-2230-2025-4-59-74.

For citation:

Larionova L.A., Sibiryak Yu.V. Obespechenie informatsionnoi bezopasnosti pri kibermoshennichestve za schet povysheniya emotsional'noi ustoichivosti pol'zovatelei [Ensuring information security against cyber fraud by increasing the emotional resilience of users]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 4 (119), pp. 59–74. DOI: 10.17212/2782-2230-2025-4-59-74.