Дата поступления рукописи в редакцию: 20.04.2026 г.
Дата принятия рукописи в печать: 27.05.2026 г.

DOI: 10.24412/2782-3849-2026-5-44-49

ГАЛУШИНА Полина Сергеевна,

старший преподаватель кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: sid-polina@yandex.ru

НЕВЕРОВА Ольга Петровна,

к.б.н., доцент кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: opneverova@mail.ru

СТЕПАНОВ Алексей Владимирович,

к.с.-х.н., доцент кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: alexeystepanow@mail.ru

ЛОПАЕВА Надежда Леонидовна,

к.б.н., доцент кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: lopaeva77@mail.ru

УКРОЖЕНКО Дарья Сергеевна,

преподаватель кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: darya.ukrozhenkozoo@mail.ru

БАРЫКИНА Екатерина Сергеевна,

преподаватель кафедры биотехнологии и пищевых продуктов, ФГБОУ ВО Уральский ГАУ,

e-mail: barykina_10@mail.ru

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В СОВРЕМЕННОМ МИРЕ: КЛЮЧЕВЫЕ ВЫЗОВЫ, СИСТЕМНЫЕ ПРОБЛЕМЫ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ

Аннотация. *В статье рассматривается социальная инженерия как одна из ключевых угроз информационной безопасности в эпоху цифровой трансформации. Анализируются методы атак, основанные на психологических манипуляциях: фишинг, вишинг, смишинг, претекстинг и другие. Показано, как развитие ИИ и расширение цифровых каналов коммуникации повышают эффективность таких атак. Описаны основные причины их успешности: недостаточная киберграмотность пользователей, когнитивные искажения, слабые внутренние регламенты организаций. Предложен комплексный подход к противодействию, включающий образовательные, организационные, технические, правовые и проактивные меры. Подчёркнута важность развития культуры кибербезопасности, международного сотрудничества и исследований в области психологии киберпреступлений для минимизации рисков в будущем.*

Ключевые слова: *социальная инженерия, информационная безопасность, киберграмотность, фишинг, вишинг, смишинг, претекстинг, искусственный интеллект, когнитивные искажения, защита данных*.

GALUSHINA Polina Sergeevna,

Senior Lecturer at the Department of Biotechnology and Food Products, Ural State Agrarian University

NEVEROVA Olga Petrovna,

Candidate of Biological Sciences, Associate Professor of the Department of Biotechnology and Food Products, Ural State Agrarian University

STEPANOV Alexey Vladimirovich,

Candidate of Agricultural Sciences, Associate Professor of the Department of Biotechnology and Food Products, Ural State Agrarian University

LOPAEVA Nadezhda Leonidovna,

Candidate of Biological Sciences, Associate Professor of the Department of Biotechnology and Food Products, Ural State Agrarian University

UKROZHENKO Darya Sergeevna,

Lecturer at the Department of Biotechnology and Food Products, Ural State Agrarian University

BARYKINA Ekaterina Sergeevna,

Lecturer at the Department of Biotechnology and Food Products, Ural State Agrarian University

SOCIAL ENGINEERING IN THE MODERN WORLD: KEY CHALLENGES, SYSTEMIC ISSUES, AND COUNTERACTION STRATEGIES

Annotation. *The article examines social engineering as a key threat to information security in the era of digital transformation. It analyses attack methods based on psychological manipulation: phishing, vishing, smishing, pretexting, and others. It shows how AI development and the expansion of digital communication channels increase the effectiveness of such attacks. The main reasons for their success are described: insufficient cyber literacy of users, cognitive biases, and weak internal regulations in organisations. A comprehensive approach to countermeasures is proposed, including educational, organisational, technical, legal, and proactive measures. The importance of developing a cybersecurity culture, international cooperation, and research in the psychology of cybercrime to minimise future risks is emphasised.*

Key words: *social engineering, information security, cyber literacy, phishing, vishing, smishing, pretexting, artificial intelligence, cognitive biases, data protection.*

В условиях интенсификации процессов цифровой трансформации общества социальная инженерия приобрела статус одной из наиболее значимых угроз информационной безопасности. В отличие от технических методов атак, эксплуатирующих уязвимости программного обеспечения и аппаратных средств, социальная инженерия целенаправленно воздействует на когнитивные и поведенческие особенности человека - наиболее уязвимое звено в системе защиты информации [1,6].

Исторически методы социальной инженерии применялись задолго до появления компьютерных технологий - в разведке, мошенничестве, психологических манипуляциях. Однако с развитием информационно коммуникационных технологий и расширением цифровой экосистемы эти методы получили принципиально новые возможности для реализации, что обусловило рост их эффективности и масштабов распространения.

Социальная инженерия в контексте информационной безопасности определяется как совокупность методов несанкционированного доступа к конфиденциальной информации или информационным системам путём манипулирования поведением человека, а не посредством технического взлома [1,6].

Ключевые механизмы воздействия базируются на глубоком понимании психологии человека. Злоумышленники создают ложное доверие, имитируя авторитетные источники - например, представляясь сотрудниками служб безопасности банков или ИТ поддержки. Они активно эксплуатируют когнитивные искажения, используя эффект срочности, когда жертве внушают необходимость немедленных действий, эффект авторитета, когда ссылка на мнимый статус повышает доверие, или эффект взаимности, когда предложение «услуги» вызывает ответное желание помочь.

Апелляция к базовым эмоциям - ещё один распространённый приём. Злоумышленники могут вызывать страх угрозой блокировки аккаунта, пробуждать любопытство заманчивыми заголовками писем или апеллировать к жадности, обещая лёгкие деньги. Кроме того, они прибегают к социальному доказательству, ссылаясь на мнимое поведение большинства или коллег, что усиливает убедительность манипуляций.

Отличие социальной инженерии от технических методов взлома заключается в том, что объектом воздействия становится не система, а человек. Методы базируются на психологии, а не на программировании, а эффективность атаки зависит от индивидуальных особенностей жертвы, а не от уровня защищённости системы [1,6].

Современные вызовы обусловлены технологическим прогрессом и изменениями в социально экономических условиях. По данным отчётов за 2023 год, более 80% киберинцидентов начинались с применения методов социальной инженерии, причём наблюдается устойчивая тенденция к усложнению сценариев атак [2].

Развитие искусственного интеллекта открыло новые возможности для злоумышленников. Нейросети позволяют генерировать персонализированные фишинговые письма, создавать убедительные дипфейки в виде поддельных аудио- и видеозаписей, а также автоматизировать подбор психологических триггеров для разных групп жертв. Расширение каналов воздействия также играет на руку преступникам: они используют социальные сети, мессенджеры, VoIP телефонию и платформы удалённой работы для проведения атак [1].

Целевые атаки, известные как «spear phishing», становятся всё более распространёнными. Направленные против конкретных организаций или высокопоставленных лиц, они требуют тщательной подготовки, но приносят злоумышленникам максимальную выгоду. Распространение дистанционных форматов работы увеличивает число потенциальных уязвимостей: сотрудники используют личные устройства для рабочих задач, отсутствует централизованный контроль безопасности, усложняется мониторинг поведения персонала.

Кроме того, развиваются и сами методы социальной инженерии. Появляются новые техники, такие как «кви про кво», когда злоумышленник предлагает помощь или услугу в обмен на доступ к системе или данным, и «дорожное яблоко», предполагающее подбрасывание заражённых носителей информации в местах скопления потенциальных жертв.

Успешность атак социальной инженерии обусловлена комплексом взаимосвязанных проблем. Прежде всего, большинство пользователей не обладают достаточными навыками распознавания признаков фишинга и других видов атак, что связано с недостаточной киберграмотностью. Во многих организациях отсутствуют чёткие правила обработки запросов на конфиденциальную информацию, что создаёт условия для злоупотреблений и свидетельствует о слабых внутренних регламентах [7].

Психологические факторы также играют значительную роль. Человеческое поведение подвержено когнитивным искажениям: люди склонны доверять авторитетам, поддаваться эффекту срочности и эмоционально реагировать на угрозы или заманчивые предложения. Систематическое обучение сотрудников вопросам кибербезопасности проводится редко, а если и проводится, то зачастую носит формальный характер, не обеспечивая реального повышения уровня защиты [5].

Технические уязвимости дополняют картину: фишинговые сайты сложно отличить от легитимных ресурсов, особенно при использовании технологий клонирования интерфейсов. Привлечение злоумышленников к ответственности затруднено из за трансграничного характера атак, сложностей идентификации преступников и несовершенства законодательства в сфере киберпреступлений. Эти правовые пробелы создают дополнительные возможности для преступной деятельности [7].

Методы атак социальной инженерии разнообразны и постоянно эволюционируют. Массовый фишинг предполагает рассылки поддельных писем большому числу адресатов с целью получения логинов, паролей или данных банковских карт. Целевой фишинг, или spear phishing, отличается тем, что атаки направлены на конкретных лиц с использованием персонализированной информации, что повышает их эффективность. Вишинг представляет собой телефонные звонки от мошенников с целью получения конфиденциальных данных, а смишинг использует SMS сообщения для тех же целей. Фарминг заключается в перенаправлении пользователей на поддельные сайты, визуально неотличимые от оригинальных [4].

Претекстинг предполагает создание ложного предлога - например, проведение опроса от имени известной компании - для получения нужной информации. Техника «кви про кво» строится на предложении помощи или услуги в обмен на доступ к системе или данным. «Плечевой серфинг» подразумевает подглядывание за экраном в общественных местах для получения паролей или другой конфиденциальной информации. «Дорожное яблоко» заключается в подбрасывании заражённых USB накопителей с интригующими надписями в местах скопления потенциальных жертв, рассчитывая на их любопытство. Кликбейт и вредоносная реклама используют заманчивые заголовки или баннеры для распространения вредоносного программного обеспечения [6].

Эффективная защита от социальной

инженерии требует комплексного подхода, включающего несколько уровней мер. Образовательные меры предполагают регулярные тренинги по кибербезопасности для сотрудников с учётом специфики их ролей, а также симуляции атак для проверки бдительности и отработки навыков реагирования. Важно проводить информационные кампании для населения с разъяснением основных угроз и методов защиты, а также внедрять программы повышения киберграмотности в образовательные стандарты [5].

Организационные меры включают разработку и внедрение политик информационной безопасности с чётким регламентом обработки запросов на конфиденциальные данные. Необходимо разграничивать доступ к информации на основе принципа минимальных привилегий, создавать процедуры верификации критически важных запросов - например, подтверждение финансовых операций по нескольким каналам - и назначать ответственных за информационную безопасность в подразделениях.

Технические меры охватывают использование антифишинговых фильтров и спам фильтров с машинным обучением для выявления подозрительных сообщений, внедрение двухфакторной аутентификации для всех критически важных систем, развёртывание систем обнаружения и предотвращения вторжений с анализом поведенческих паттернов. Мониторинг подозрительной активности с использованием алгоритмов искусственного интеллекта и регулярное обновление программного обеспечения для устранения уязвимостей также играют важную роль [6].

Правовые и регуляторные меры должны предусматривать ужесточение законодательства в сфере киберпреступлений с введением более строгих санкций, развитие международного сотрудничества в борьбе с киберпреступностью, включая обмен информацией и координацию расследований, а также стандартизацию требований к информационной безопасности в организациях различных секторов [7].

Проактивные меры предполагают проведение пентестов с элементами социальной инженерии для выявления уязвимостей, аудит безопасности и оценку рисков с учётом человеческого фактора, разработку сценариев реагирования на инциденты с участием социальной инженерии и создание центров мониторинга и реагирования на киберинциденты.

Эволюция методов социальной инженерии предполагает дальнейшее развитие искусственного интеллекта и машинного обучения для создания более убедительных дипфейков и персонализированных атак. Использование больших данных позволит анализировать поведение потенциальных жертв и подбирать оптимальные методы воздействия. Появление новых каналов воздействия, связанных с развитием метавселенных и технологий виртуальной реальности, создаст дополнительные угрозы. Рост сложности атак потребует междисциплинарного подхода к защите, объединяющего знания в области психологии, информационных технологий, права и социологии [3].

Для эффективного противодействия необходимо развивать адаптивные системы защиты, способные обучаться на новых типах атак, интегрировать методы поведенческого анализа в системы кибербезопасности, формировать культуру кибербезопасности на уровне общества и стимулировать научные исследования в области психологии киберпреступлений и методов противодействия им [1,7].

Социальная инженерия остаётся одной из наиболее опасных угроз информационной безопасности, поскольку эксплуатирует фундаментальные особенности человеческого поведения, которые сложно устранить техническими средствами. Основные вызовы связаны с технологическим прогрессом, глобализацией и изменениями в образе жизни людей. Системные проблемы кроются в недостаточной киберграмотности, слабых регламентах, психологических факторах и правовых пробелах [1,7].

Эффективная стратегия противодействия требует комплексного подхода: сочетания образовательных, организационных, технических, правовых и проактивных мер. Для минимизации рисков необходимо повышать киберграмотность населения, внедрять современные технические решения, совершенствовать законодательство и развивать международное сотрудничество.

Дальнейшие исследования в области противодействия социальной инженерии должны быть сосредоточены на разработке адаптивных систем защиты, способных оперативно реагировать на эволюцию методов атак. Особое внимание следует уделить интеграции поведенческого анализа в существующие системы кибербезопасности: такой подход позволит выявлять подозрительные паттерны действий на ранних стадиях и предотвращать инциденты до их реализации.

Изучение психологических механизмов, лежащих в основе успешности атак социальной инженерии, представляет собой важное направление научных изысканий. Понимание когнитивных искажений, эмоциональных триггеров и социально психологических факторов, влияющих на принятие решений,

открывает возможности для создания более эффективных образовательных программ и инструментов защиты. К примеру, результаты исследований в области когнитивной психологии могут лечь в основу методик тренировки критического мышления у сотрудников организаций, что повысит их устойчивость к манипуляциям.

Развитие технологий искусственного интеллекта обладает значительным потенциалом для противодействия атакам социальной инженерии. Алгоритмы машинного обучения, обученные на обширных массивах данных о предыдущих инцидентах, способны автоматически выявлять признаки фишинговых писем и сообщений, анализировать поведенческие паттерны пользователей для обнаружения аномалий, прогнозировать наиболее вероятные векторы атак на основе анализа открытых источников информации о компании, а также создавать симуляционные модели для обучения персонала с учётом актуальных угроз.

Формирование культуры кибербезопасности на уровне общества выступает не менее значимым аспектом. Это подразумевает внедрение программ киберграмотности в систему общего и профессионального образования, проведение регулярных информационных кампаний для населения через СМИ и социальные сети, создание общедоступных ресурсов с актуальной информацией о методах социальной инженерии и способах защиты, а также популяризацию принципов цифровой гигиены среди всех возрастных групп.

Международное сотрудничество в сфере противодействия киберпреступности требует особого внимания ввиду трансграничного характера атак социальной инженерии. Развитие механизмов обмена информацией между правоохранительными органами разных стран, унификация законодательства в сфере кибербезопасности, координация усилий по расследованию сложных случаев, затрагивающих несколько юрисдикций, и совместная разработка стандартов защиты от атак социальной инженерии для критически важных инфраструктур - всё это критически важно для эффективной борьбы с угрозой.

Список литературы:

[1] Диреев, И. Д. Социальная инженерия в контексте информационной безопасности / И. Д. Диреев // Международный научно-исследовательский журнал. – 2025. – № 3(153). – DOI 10.60797/IRJ.2025.153.121. – EDN APZMDR.

[2] Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть пятая [Электронный ресурс] / Positive Technologies. - URL: https://ptsecurity.com/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (дата обращения: 19.04.2026).

[3] Кюнер, А. П. Обзор научных работ по социальной инженерии / А. П. Кюнер, А. А. Чечулин // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2025. – № 4. – С. 94-106. – DOI 10.61260/2218-130X-2025-4-94-106. – EDN TXAIGE.

[4] МСЭ Т представил международные стандарты для борьбы с телефонным мошенничеством [Электронный ресурс] // ComNews. - 26.06.2025. - URL: https://www.comnews.ru/content/239859/2025-06-26/2025-w26/1007/mse-t-predstavil-mezhdunarodnye-standarty-dlya-borby-telefonnym-moshennichestvom (дата обращения: 19.04.2026).

[5] Панилов, П. А. Когнитивный центр кибербезопасности критической инфраструктуры: гибридный подход с использованием графовых моделей и эволюционных алгоритмов / П. А. Панилов // Национальная безопасность и стратегическое планирование. – 2024. – № 3(47). – С. 55-67. – DOI 10.37468/2307-1400-2024-3-55-67. – EDN DPFQUK.

[6] Рейн, Т. С. Основы социальной инженерии в компьютерной безопасности : учебное пособие / Т. С. Рейн. - Кемерово : КемГУ, 2025. - 99 с. - ISBN 978-5-8353-3309-7. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/495473 (дата обращения: 19.04.2026). - Режим доступа: для авториз. пользователей.

[7] Черецких, А. В. Противодействие негативным методам социальной инженерии / А. В. Черецких // Виктимология. – 2023. – Т. 10, № 4. – С. 474-484. – DOI 10.47475/2411-0590-2023-10-4-474-484. – EDN JYCREI.

References:

[1] Direev, I. D. Social Engineering in the Context of Information Security/I. D. Direev// International Research Journal. – 2025. – № 3(153). – DOI 10.60797/IRJ.2025.153.121. – EDN APZMDR.

[2] Cybersecurity 2023-2024: Trends and Forecasts. Part Five [Electronic Resource]/ Positive Technologies. - URL: https://ptsecurity.com/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (дата обращения: 19.04.2026).

[3] K ner, A. P. Review of scientific works on social engineering/A. P. K ner, A. A. Chechulin// Scientific and analytical journal “Bulletin of St. Petersburg University of the State Fire Service of the

Ministry of Emergencies of Russia." – 2025. – № 4. - S. 94-106. – DOI 10.61260/2218-130X-2025-4-94-106. – EDN TXAIGE.

[4] ITU T presented international standards for combating telephone fraud [Electronic Resource]//ComNews. - 26.06.2025. - URL: https://www.comnews.ru/content/239859/2025-06-26/2025-w26/1007/mse-t-predstavil-mezhdunarodnye-standarty-dlya-borby-telefonnym-moshennichestvom (дата обращения: 19.04.2026).

[5] Panilov, P. A. Cognitive Center for Cybersecurity of Critical Infrastructure: A Hybrid Approach using Graph Models and Evolutionary Algorithms/P. A. Panilov//National Security and Strategic Planning. – 2024. – № 3(47). - S. 55-67. – DOI 10.37468/2307-1400-2024-3-55-67. – EDN DPFQUK.

[6] Raine, T. S. Fundamentals of Social Engineering in Computer Security: A Study Guide/T. S. Raine. - Kemerovo: KemSU, 2025. - 99 p. - ISBN 978-5-8353-3309-7. - Text: electronic//Doe: electronic library system. - URL: https ://e.lanbook.com/book/495473 (accessed: 19.04.2026). - Access mode: for authoring. users.

[7] Cheretsky, A.V. Counteraction to negative methods of social engineering/A.V. Cheretsky// Victimology. – 2023. - T. 10, NO. 4. - S. 474-484. – DOI 10.47475/2411-0590-2023-10-4-474-484. – EDN JYCREI.