

Научная статья

УДК 159.9

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ЭПОХУ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: РЕСУРСЫ И УЯЗВИМОСТИ ПРИ
ВЗАИМОДЕЙСТВИИ С ИНТЕРНЕТ-СРЕДОЙ

Георгий Павлович Гензе¹, Елена Леонидовна Солдатова²

^{1, 2} Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

¹ mr.genze@gmail.com

² elena.l.soldatova@gmail.com

Аннотация. В условиях цифровой трансформации, когда каждый сотрудник независимо от профессиональной позиции становится оператором информационной системы, фишинговые атаки становятся критической эргономической угрозой в системе «человек-информация-среда». Особую актуальность данная проблема приобретает для образовательных учреждений, обеспечивающих подготовку кадров для оборонно-промышленного комплекса, где человеческий фактор выступает наиболее уязвимым звеном в системе защиты. Целью представленного в статье исследования является теоретическое обоснование и разработка интегративной психосоциальной модели уязвимости к фишинговым атакам, адаптированной к организационно-поведенческим характеристикам данных учреждений.

На основе компаративного анализа современных зарубежных и отечественных исследований идентифицированы шесть ключевых блоков факторов уязвимости: когнитивные искажения, эмоциональные состояния, социально-демографические характеристики, индивидуально-личностные черты, поведенческие паттерны и уровень цифровой грамотности. Предложена математическая модель оценки уязвимости, реализованная в форме логистической регрессии, которая позволяет на основе данных валидизированных психометрических методик осуществлять классификацию пользователей по степени риска подверженности фишингу.

Установлено, что уязвимость детерминируется не изолированными факторами, а их системным взаимодействием. При этом определяющее значение приобретают специфика когнитивных искажений, эмоциональная регуляция в стрессовых условиях, особенности мотивации к защите, а также поведенческие стереотипы, характерные для сотрудников и обучающихся. Рассмотрены преимущества и ограничения применения регрессионного моделирования, а также проанализированы противоречия в существующих эмпирических данных. Полученные результаты могут быть использованы при разработке дифференцированных программ повышения цифровой грамотности и формирования компетенций кибергигиены.

Ключевые слова: фишинговые атаки, уязвимость пользователя, человеческий фактор, когнитивная эргономика, цифровая грамотность, логистическая регрессия, образовательная среда, кибербезопасность

Для цитирования: Гензе Г.П., Солдатова Е.Л. Человеческий фактор в эпоху социальной инженерии: ресурсы и уязвимости при взаимодействии с интернет-средой // Вестник Военной академии войск национальной гвардии. 2026. № 3 (36). С.103–113. URL: <http://vestnik-academrg.ru/2026/09/011.pdf>.

WORK PSYCHOLOGY, ENGINEERING PSYCHOLOGY, COGNITIVE ERGONOMICS

Original article

THE HUMAN FACTOR IN THE AGE OF SOCIAL ENGINEERING: RESOURCES AND VULNERABILITIES IN
INTERACTING WITH THE INTERNET ENVIRONMENT

Georgy P. Genze¹, Elena L. Soldatova²

^{1, 2} Saint Petersburg State University, Saint Petersburg, Russia,

¹ mr.genze@gmail.com

² elena.l.soldatova@gmail.com

Abstract. In the context of the digital transformation of the educational environment, phishing attacks are becoming a critical threat to information security. This problem is particularly relevant

for educational institutions training personnel for the military-industrial complex and those involved with state secrets, where the human factor is the most vulnerable link in the security system. The aim of this article is to theoretically substantiate and develop an integrative psychosocial model of vulnerability to phishing attacks, applicable to the specific characteristics of these institutions.

Based on a comparative analysis of modern international and domestic studies, six key vulnerability factors are identified: cognitive biases, emotional states, socio-demographic characteristics, individual personality traits, behavioral patterns, and digital literacy. A mathematical vulnerability assessment model, implemented in the form of logistic regression, is proposed. This model, based on data from validated psychometric methods, allows for the classification of users according to their risk of exposure to phishing. It has been established that vulnerability is determined not by isolated factors, but by their systemic interactions. Specific cognitive biases, emotional regulation under stress, protective motivation, and persistent behavioral patterns characteristic of employees and students at restricted-access educational institutions are crucial. The advantages and limitations of regression modeling are examined, and inconsistencies in existing empirical data are analyzed. The findings can be used in the development of differentiated programs to improve digital literacy and develop cyber hygiene competencies, taking into account the confidential nature of the activities.

Keywords: phishing attacks, user vulnerability, human factor, digital literacy, logistic regression, educational environment, cybersecurity

For citation: Genze G.P., Soldatova E.L. The human factor in the age of social engineering: resources and vulnerabilities in interacting with the internet environment. *Vestnik Voennoj akademii vojsk nacional'noj gvardii*. 2026;3(36): 103–113. (In Russ.). Available from: <http://vestnik-academrg.ru/2026/09/011.pdf>.

© Гензе Г.П., Солдатова Е.Л., 2026

Введение

В условиях цифровизации профессиональной деятельности критическое мышление и цифровая бдительность становятся важными качествами специалистов, работающих с информацией. Особенно уязвима образовательная среда, где коммуникация часто маскируется под легитимные сообщения. Фишинг следует рассматривать не только как техническую, но и как психологическую проблему, связанную с особенностями электронной деятельности. Расширение дистанционных и гибридных форм обучения усиливает данные риски.

Несмотря на развитие технических средств защиты, значительная часть уязвимости обусловлена человеческим фактором – совокупностью когнитивных, эмоциональных и социально-психологических характеристик индивида, которые определяют его предрасположенность к небезопасным действиям в условиях социально-инженерных атак.

Уязвимостью пользователя называется характеристика индивида, выражающаяся в повышенной вероятности стать жертвой социально-инженерной атаки при взаимодействии с интернет-средой.

С 2020 по 2025 г. фишинговые атаки демонстрируют устойчивый рост и усложнение. По данным Anti-Phishing Working Group, только во втором квартале 2025 г. зафиксировано более 1 млн атак [2]. В отчёте Data Breach Investigations Report 2025 со-

циальная инженерия и фишинг стабильно входят в число ведущих причин утечек данных [13; 38].

Современные атаки используют принципы юзабилити-дизайна, вызывая когнитивный конфликт и вынуждая действовать быстро в режиме многозадачности. Применяются персонализированные сценарии (spear-phishing), генеративный искусственный интеллект, deepfake-материалы, QR-фишинг. Сектор образования в 2023 г. вошёл в число наиболее атакуемых: университеты становятся мишенью из-за большого числа учётных записей и ценности академической информации [35].

Эмпирические исследования показывают высокую вероятность совершения целевого действия среди студентов – в тестовых рассылках до 50 % переходов по ссылкам. Преподаватели чаще становятся объектом целевых атак. Низкие показатели репортирования о фишинге (10–20 %) подтверждают высокий риск [28].

Уязвимость связана с её открытым характером, а также с создаваемыми ею условиями информационной перегрузки и высокой психологической нагрузки на пользователей. Дополнительными факторами выступают профессиональное выгорание преподавателей и академический стресс студентов.

В современной литературе (с 2020 г.) преобладают работы, посвящённые анализу когнитивных искажений и поведенческих факторов [10; 21; 36; 42], однако заме-

тен дефицит исследований, направленных на разработку математических моделей уязвимости конкретных групп пользователей.

Цель – проанализировать научную литературу по проблемам киберугроз в образовательном пространстве и выявить психологические факторы, влияющие на уязвимость субъектов образовательной среды (студентов и преподавателей) к фишингу.

Анализ исследований проблематики фишинга

Фишинг – вид интернет-мошенничества, при котором злоумышленники посредством поддельных писем или веб-ресурсов стремятся получить конфиденциальные данные либо побудить к загрузке вредоносного ПО.

Исследование Фана и соавт. (Fan et al., 2023) выявило детерминанты фишинговой уязвимости с использованием объяснимого искусственного интеллекта [18]. Авторы применяли личностно-ориентированную модель, опросники («Большая пятёрка», шкала воспринимаемого стресса) и смулированную фишинговую кампанию. Нейросетевая модель показала точность 78 % при полноте 71 %.

Систематический обзор Десольда и соавт. (Desolda et al., 2022) обобщает исследования, анализируя влияния факторов [15]:

1. Модификация пользовательского интерфейса (User Interface).
2. Отношение пользователей и психологические аспекты (Attitude, Behaviour, Psychological Aspects).
3. Обучение пользователей (Knowledge, Education, Training).
4. Структуры для дизайнеров (Framework, Models, Taxonomies).

Авторы выделяют психологические предикторы: импульсивность шкала (BIS-11), рискованное онлайн-поведение (RScB), установки к кибербезопасности (CAS), осведомлённость (ISAS), воспринимаемый риск (PMT, TPB), когнитивные тесты (CRT), эмоциональные состояния (PSS, STAI), социальные нормы (TPB). Выявлены пробелы: недостаток данных по фишингу в образовательной среде, неясность когнитивных механизмов в больших языковых моделях (LLM), слабая изученность мультимодальных атак.

Кортеллинг и соавт. (Korteling et al., 2023) предлагают нейросетевую модель для объяснения когнитивных искажений, показывая, что мозг систематически склоняется к эвристическому принятию решений, и аргу-

ментируют, что многие когнитивные искажения возникают из внутренних механизмов мозга, фундаментальных для работы биологических нейронных сетей [24].

Исследование Джаятилака и соавт. (Jayatilaka et al., 2024) предлагает качественную модель принятия решений при взаимодействии с фишинговыми письмами, включающую этапы восприятия, интерпретации, оценки срочности и доверия [21; 33].

Хан и соавт. (Khan et al., 2022) проанализировали эффективность тренингов, опираясь на теоретически обоснованные показатели модели Киркпатрика [23]. Показано, что повышение осведомлённости не всегда приводит к устойчивым поведенческим изменениям.

Исследование Вишваната и соавт. (Vishwanath et al., 2018) представляет модель SCAM (Suspicion, Cognition, and Automaticity Model) [40], включающую три компонента:

- Suspicion (подозрительность) – способность распознать подозрительные признаки.
- Cognition (когнитивная обработка) – осознанный анализ при активации подозрительности.
- Automaticity (автоматизм) – поведенческие привычки.

Результаты показали, что:

1. Автоматичность (независимая переменная) выступает ключевым предиктором уязвимости (зависимая переменная).
2. Подозрительность выполняет функцию медиатора в отношении связи между когнитивной нагрузкой и успешностью распознавания фишинга (или: между автоматичностью и уязвимостью — выбрать нужное).
3. Знания о фишинге слабо коррелируют с фактической защищённостью, что указывает на разрыв между когнитивной осведомлённостью и поведенческой реализацией.

Спадаро и соавт. (Spadaro et al., 2023) показали, что восприятие честности социального окружения влияет на готовность к кооперации и чувствительность к манипуляциям [37].

Хэдлинтон и соавт. (Hadlington et al., 2017) выявили индивидуальные предикторы рискованного онлайн-поведения [20]: импульсивность (BIS-11), интернет-зависимость (IAT), установки к кибербезопасности (CAS), рискованное поведение (RScB). Импульсивность – наиболее сильный предиктор.

Ван и соавт. (Wang et al., 2021) анализируют уязвимость через модель когнитивных искажений с акцентом на эффект избыточной уверенности [41]. Компоненты предвзятости самоуверенности показали высокую взаимосвязь ($r=0,628$).

Марин и соавт. (Marin et al., 2023) изучали намерение сообщать о фишинге на основе теории запланированного поведения [27]. Методика включала предъявление сценариев, оценку риска, фиксацию поведенческого намерения, измерение установок, субъективных норм и воспринимаемого контроля.

В обзоре Альмансуури и соавт. (Almansoori et al., 2023) систематизированы психологические модели: человеческий фактор, рискованное поведение, когнитивная нагрузка, мотивация защиты [12].

Патель и соавт. (Patel et al., 2024) сравнили когнитивное распознавание угроз с LLM-моделями [31]. Показано, что и люди, и модели подвержены ошибкам при наличии психологических стимулов в письмах (срочности, страха, социальной значимости).

Шэн и соавт. (Sheng et al., 2010) выявили демографические факторы восприимчивости к фишингу и оценили эффективность обучающих программ [25].

Совокупный анализ показывает многомерный характер психологической уязвимости, охватывающей личностные, поведенческие особенности и когнитивные процессы.

Определение видов факторов уязвимости

На основе анализа исследований выделены шесть блоков факторов:

1. Когнитивные факторы

Включают способность к анализу, когнитивные искажения, внимательность. Пользователи с низкой аналитической активностью чаще поддаются социально-инженерному воздействию [21; 33]. Выявлены: ошибки обработки информации [15; 20; 21; 31; 33], когнитивные искажения [24; 36; 39; 41], снижение аналитической обработки [21; 31; 33], ограниченность рабочей памяти [12; 15], ошибочная оценка угроз [23; 27; 39; 41].

2. Эмоциональные факторы

Отражают усталость, реактивность, восприимчивость к стимулам [3; 9; 30]; включают тревожность и стресс [12; 15; 23]; страх и срочность [21; 23; 33]; эмоциональную нестабильность [20; 37]; снижение доверия [37]. Эмоциональные факторы усиливают когнитивную уязвимость [29].

3. Социально-демографические факторы

К данной группе относятся возраст, уровень образования, цифровой опыт и особенности социального контекста [1; 8; 19]. Эти параметры не выступают прямыми причинами уязвимости, но опосредованно влияют на сформированность навыков распознавания угроз, стратегии обработки информации и поведенческие реакции в цифровой среде [25; 27; 34]. Возраст и образовательный уровень [12; 15], а также организационная среда [27] и социальное окружение [37] задают условия, в которых формируются либо ресурсы безопасности, либо дополнительные риски.

4. Индивидуально-личностные факторы

Включают самооффективность, мотивацию к защите, склонность к риску [4; 6; 32], уровень доверчивости [18; 37], импульсивность [12; 15; 20] и особенности самооффективности [23; 27], привычные стратегии [24; 31] и самооценки [31; 36; 41]. Эти характеристики определяют, каким образом пользователь воспринимает цифровые угрозы, оценивает собственные возможности и принимает решения. Индивидуальные особенности формируют когнитивные и эмоциональные реакции на потенциально опасные сообщения и, соответственно, повышают или снижают вероятность ошибочных действий.

5. Поведенческие факторы

Связаны с устойчивыми паттернами цифрового поведения: автоматизированными действиями [18; 20; 21; 33] при работе с письмами, склонностью к импульсивной активности пользователя [16; 17; 22], привычкой открывать подозрительные сообщения [15; 21; 33] или игнорировать процедуры проверки. К этой группе также относится готовность сообщать о фишинговых инцидентах [23; 27] и точность классификации писем [31; 36; 41]. Поведенческие привычки отражают степень сформированности защитных стратегий либо закреплённых рискованных моделей взаимодействия [12; 20].

6. Цифровая грамотность

Представляет собой совокупность знаний о киберугрозах и практических навыков безопасной работы в сети [5; 7; 14]. Уязвимость повышается при недостаточной способности распознавать признаки фишинга [18; 20; 21; 33; 36; 41], неполном понимании процедур [12; 23; 27] безопасности и расхождении между субъективной уверенностью и реальным

уровнем компетентности [36; 41]. Таким образом, цифровая грамотность выступает ключевым ресурсом, модифицирующим влияние других факторов риска.

Анализ противоречий в исследуемых моделях

Современные исследования демонстрируют неоднозначность в оценке роли ключевых предикторов уязвимости к фишингу.

Во-первых, выявляется диссонанс между декларируемыми знаниями правил кибербезопасности и реальными поведенческими паттернами: хотя обучающие программы повышают осведомлённость пользователей [12], наличие знаний само по себе не гарантирует корректных действий в реальной ситуации угрозы [18]. Это указывает на опосредованный характер влияния когнитивной компетентности и необходимость учитывать поведенческие и ситуационные механизмы [11; 26; 33; 40].

Во-вторых, доверие выполняет двойственную функцию [15]. Доверие к организации может усиливать готовность соблюдать правила и сообщать о фишинговых инцидентах, тогда как доверие к конкретному отправителю сообщения повышает риск ошибочного взаимодействия [21]. Таким образом, эффект доверия зависит от его направленности и контекста.

В-третьих, влияние социально-демографических характеристик оказывается неоднозначным. Возраст и уровень образования редко выступают самостоятельными детерминантами уязвимости [25], чаще отражая различия в цифровом опыте и условиях взаимодействия с интернет-средой.

Наконец, самооэффективность может играть как защитную, так и рискованную роль: адекватная уверенность способствует соблюдению мер безопасности, тогда как избыточная уверенность (overconfidence) снижает критическую настороженность [34].

Выявленные противоречия во многом обусловлены методологическими различиями исследований – использованием разных инструментов измерения одних и тех же конструктов, особенностями выборок и временным дизайном. Это подтверждает необходимость интегративного подхода к анализу психологических ресурсов и уязвимости в цифровой среде.

Применение анализа в гипотетической модели

Анализ показывает отсутствие единой универсальной модели уязвимости. Выявленные противоречия указывают на многофакторную природу уязвимости.

Рекомендации по построению гипотетической модели:

1. Многоуровневый анализ с учётом индивидуальных и организационных факторов
2. Мета-анализ по ключевым эффектам
3. Долгосрочные эксперименты
4. Прописать в модели набор блоков

Гипотетическая модель

Модель основывается на предположении, что уязвимость определяется совокупным влиянием 6 факторов:

1. Когнитивные факторы (Cog) – способность к анализу, критическое мышление, когнитивные искажения.
2. Эмоциональные факторы (Emot) – восприимчивость к стрессу, усталости, эмоциональным стимулам.
3. Социально-демографические факторы (SocD) – возраст, цифровой опыт, образование, социальные нормы.
4. Индивидуально-личностные факторы (Pers) – самооэффективность, мотивация к защите, склонность к риску.
5. Поведенческие факторы (Beh) – привычки работы с письмами, импульсивность.
6. Цифровая грамотность (DG) – знания о цифровой безопасности.

Математизация гипотетической модели

Для построения модели используется логистическая регрессия:

$$\text{vuln} = 1 / (1 + \exp(-z)),$$

$$\text{где } z = a_0 + a_1 \cdot \text{Cog} + a_2 \cdot \text{Emot} + a_3 \cdot \text{SocD} + a_4 \cdot \text{Pers} + a_5 \cdot \text{Beh} + a_6 \cdot \text{DG} + \varepsilon.$$

Cog – склонность к аналитическому мышлению (Cognitive Reflection Test), мотивация к глубокой переработке (Need for Cognition Scale), тест внимания d2.

Emot – уровень стресса (Perceived Stress Scale), восприимчивость к угрозам (State-Trait Anxiety Inventory).

SocD – возраст, образование, цифровой опыт, давление со стороны коллег.

Pers – самооэффективность (Self-Efficacy Scale), склонность к риску (Risk-Taking Scale), доверие (Trust measures).

Beh – частота небезопасных действий (Risky Cybersecurity Behaviours Scale), импульсивность (Barratt Impulsiveness Scale).

DG – знания о безопасности (Information Security Awareness Scale), установки (Cybersecurity Attitudes Scale).

$a_0, a_1, \dots, a_6$ – параметры модели, ε – случайная ошибка.

Классификация на уязвимых (0) и уязвимых (1) через пороговое значение p :

- $y = 0$, если $\text{vuln} < p$
- $y = 1$, если $\text{vuln} \geq p$

Оптимальное p определяется через ROC-кривую и AUC. Параметры оцениваются максимизацией функции правдоподобия.

Характеристика гипотетической модели
Преимущества:

1. Интерпретируемость – модель позволяет выявить и содержательно описать значимые предикторы уязвимости (например, уровень тревожности, склонность к автоматическим реакциям) с указанием направления и силы их влияния.

2. Бинарная классификация – модель прогнозирует принадлежность индивида к одному из двух классов: «уязвимый» или «резистентный» к фишинговой атаке, что даёт чёткое практическое правило для прогнозирования.

3. Гибкость – допускает одновременное включение количественных (возраст, время реакции) и категориальных (пол, тип занятости) переменных без дополнительного преобразования шкал.

4. Статистическая оценка значимости – каждый предиктор сопровождается p -значением и доверительным интервалом, что позволяет отсеивать случайные связи.

Недостатки:

1. Линейная зависимость логитов – модель предполагает линейную связь между логитом вероятности и предикторами, что не позволяет полностью учесть нелинейные взаимодействия (например, синергетический эффект двух факторов).

2. Чувствительность к мультиколлинеарности – при высокой корреляции между предикторами оценки коэффициентов становятся нестабильными, что требует предварительного отбора переменных.

3. Необходимость ручного добавления взаимодействий – в отличие от деревьев решений или нейросетей, модель не автоматически обнаруживает эффекты взаимодействия; их нужно задавать исследователем вручную.

4. Ограниченная способность к предсказанию редких событий – при малой доле уязвимых в выборке модель может давать смещённые оценки.

5. Отсутствие динамики – фиксация состояния на момент опроса – модель фиксирует состояние на момент опроса и не отражает изменения уязвимости во времени (например, после тренинга).

Открытые задачи:

1. Определение оптимального порогового значения p

2. Выбор наиболее информативного набора психометрических тестов

3. Проверка валидности на независимых выборках студентов и преподавателей

Модель объединяет математическую строгость логистической регрессии с психологической валидностью выбранных факторов и позволяет формально оценивать вероятность уязвимости каждого респондента.

Заключение

Проведённый теоретический анализ позволил выделить ключевые психологические факторы уязвимости на когнитивном, эмоциональном и социально-демографическом уровнях. Учитывая, что в условиях повышенных требований к конфиденциальности и режиму секретности, важно своевременно выявлять зоны потенциального риска, в том числе оценивая такие индивидуально-личностные особенности как критическое мышление и опыт распознавания угроз. Дополнительные векторы уязвимости: тревожность, страх упустить значимую информацию ведомственного характера и социальное давление в закрытых коммуникационных контурах. Доверие к вышестоящим инстанциям и влияние профессионального окружения тоже формируют зоны критического риска, тогда как возрастные характеристики, опыт работы с конфиденциальными данными и уровень специализированной цифровой грамотности определяют индивидуальные различия в восприимчивости к социотехническим угрозам.

Разработка математической модели, учитывающей теоретически выявленные параметры, требует ее эмпирической проверки на целевых группах респондентов.

Практическая значимость работы заключается в том, что предложенные и валидизированные модели могут служить основой для ведомственных образовательных программ в области кибербезопасности. Приоритетными направлениями в рамках таких программ следует считать развитие критического мышления в условиях информационной закрытости, формирование эмоциональной саморегуляции при взаимодействии с чувствительными данными, а также закрепление паттернов осознанного цифрового поведения в защищённых сегментах интернет-среды.

Список источников

1. Джусупова Р. А. Влияние морального и правового сознания на социальное поведение // Bulletin of the Academy of Justice. 2025. DOI: 10.63546/3005-2246.2025.10.2.002.
2. Ландшафт угроз для систем промышленной автоматизации. Европа. II квартал 2025 года. URL: <https://ics-cert.kaspersky.ru/publications/reports/2025/09/11/threat-landscape-for-industrial-automation-systems-q2-2025>.
3. Лобанова Е. В. Социологический анализ влияния корпоративной культуры на эффективность обучения в технических университетах / Е. В. Лобанова, Г. П. Сапожников // Modern scientist. 2024. № 7. С. 353–367.
4. Моросанова В. И. Диагностика устойчивости психической саморегуляции в напряженных условиях в ситуации эксперимента / В. И. Моросанова, В. Н. Красников // Экспериментальная психология. 2012. Т. 5, № 4. С. 44–53.
5. Нестик Т. А. Социально-психологические предпосылки и типы долгосрочной ориентации: результаты эмпирического исследования // Психологический журнал. 2021. Т. 42, № 4. С. 28–39. DOI: 10.31857/S020595920016008-4.
6. Прохоров А. О. Динамика ментальной регуляции психических состояний студентов в различных условиях учебной деятельности / А. О. Прохоров, А. В. Чернов, М. Г. Юсупов // Экспериментальная психология. 2024. Т. 17, № 3. С. 130–143. DOI: 10.17759/exppsy.2024170309.
7. Солдатова Г. У. Цифровое поколение России: компетентность и безопасность / Г. У. Солдатова, Е. И. Рассказова, Т. А. Нестик. М.: Смысл, 2017. 375 с.
8. Сташкова Т. В. Психологические аспекты моделирования профессионально-личностного развития педагога в системе повышения квалификации // Инновационная наука психология педагогика дефектология. 2021. Т. 4, № 3. С. 55–64. DOI: 10.23947/2658-7165-2021-4-3-55-64.
9. Фабрикант М. С. Психологические факторы кибербезопасности и доверие к ложным новостям в интернет-коммуникации: обзор современных зарубежных исследований // Современная зарубежная психология. 2024. Т. 13, № 4. С. 163–171. DOI: 10.17759/jmfp.2024130415.
10. Abroshan H., Devos J., Poels G., Laermans E. COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic // IEEE Access. 2021. Vol. 9. P. 121–130. DOI: 10.1109/ACCESS.2021.3109091.
11. Agagu M., Omorogiwa O. Investigating and Mitigating User Susceptibility to Phishing Using the Analysis of Demographic Information, Knowledge and Cognitive Experience. Advances in Multidisciplinary & Scientific // Research Journal Publication. 2019. Vol. 13, no. 2. P. 94–107. DOI: 10.22624/AIMS/BHI/V11N2P8.
12. Almansoori A., Al-Erman M., Shaalan K. Exploring the frontiers of cybersecurity behavior: A systematic analysis // Applied Sciences. 2023. Vol. 13, no. 9. P. 5700. DOI: 10.3390/app13095700.
13. Bitaab M., Cho H., Oest A., Zhang P. Scam pandemic: How attackers exploit public fear through phishing // Conference: 2020 APWG Symposium on Electronic Crime Research. DOI: 10.48550/arXiv.2103.12843.
14. Caputo D. D., Pfleeger S. L., Freeman J. D., Johnson M. E. Going spear phishing: Exploring embedded training and awareness // IEEE Security and Privacy Magazine. 2014. Vol. 12, no. 1. P. 28–38. DOI: 10.1109/MSP.2013.106.
15. Desolda G., Ferro L. S., Marrella A., Costabile M. F., Catarci T. Human Factors in Phishing Attacks: A Systematic Literature Review // ACM Computing Surveys (CSUR). 2022. Vol. 54, no.8. P. 1–35. DOI: 10.1145/3469886.
16. Diaz A., Sherman A. T., Joshi A. Phishing in an academic community: A study of user susceptibility and behavior // Cryptologia. 2019. Vol. 44, no. 1. P. 1–15. DOI: 10.48550/arXiv.1811.06078.
17. Falade P. V. Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks // International Journal of Scientific Research in Computer Science Engineering and Information Technology. 2023. Vol. 9, no. 5. P. 185–198. DOI: 10.32628/CSEIT2390533.
18. Fan Z., Li W., Laskey K. B., Chang K. C. Investigation of phishing susceptibility with explainable artificial intelligence // MDPI. 2023. Vol. 16, no. 1. DOI: 10.20944/preprints202311.1540.v1.
19. Furnell S., Shah N. J. Home working and cyber security – an outbreak of unpreparedness? // Computer Fraud & Security. 2020. no. 8. P. 6–12. DOI: 10.1016/s1361-3723(20)30084-1.

20. Hadlington L. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviours // *Heliyon*. 2017. Vol. 3, no. 7. DOI: 10.1016/j.heliyon.2017.e00346.
21. Jayatilaka A., Arachchilage N. A. G., Babar M. A. Why people still fall for phishing emails: An empirical investigation into how users make email response decisions // *Symposium on Usable Security*. 2024. DOI: 10.14722/usec.2024.23072.
22. Kashapov A., Wu T., Abuadbbba S., Rudolph C. Email summarization to assist users in phishing identification // *Conference: ASIA CCS '22: ACM Asia Conference on Computer and Communications Security*. 2022. DOI: 10.48550/arXiv.2203.13380.
23. Khan N. F., Ikram N., Murtaza H., Javed M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model // *Computers & Security*. 2022. Vol. 125. P. 7–8. DOI: 10.1016/j.cose.2022.103049.
24. Korteling J. E., Paradies G. L., Sassen-van Meer J. P. Cognitive bias and how to improve sustainable decision making // *Front. Psychol., Sec. Cognitive Science*. 2023. Vol. 14. DOI: 10.3389/fpsyg.2023.1129835.
25. Kumaraguru P., Sheng S., Acquisti A., Cranor L. Teaching Johnny not to fall for phish // *ACM Transactions on Internet Technology*. 2010. Vol. 10, no. 2. DOI: 10.1145/1754393.1754396.
26. Malloy T., Ferreira M. J., Fang F., Gonzalez C. Leveraging a cognitive model to measure subjective similarity of human and GPT-4 written content // *Conference: Proceedings of the 28th Conference on Computational Natural Language Learning*. 2024. DOI: 10.48550/arXiv.2409.00269.
27. Marin I. A., Burda P., Zannone N., Allodi L. The influence of human factors on the intention to report phishing emails // *Conference: CHI '23: CHI Conference on Human Factors in Computing Systems*. 2023. No. 20. P. 1–18. DOI: 10.1145/3544548.3580985.
28. Morrow E. Scamming higher ed: An analysis of phishing content and trends // *Computers in Human Behavior*. 2024. Vol. 158, no. 3. DOI: 10.1016/j.chb.2024.108274.
29. Mousa J. An overview of phishing victimization: Human factors, training and the role of emotions // *Computer Science & Information Technology*. 2022. Vol. 12, no. 13. P. 197–207. DOI: 10.5121/csit.2022.121319.
30. Nagar P. The Psychology of Cyber Fraud: Unraveling the Tactics Behind Modern-Day Scams // *The International Journal of Indian Psychology*. 2025. Vol. 13, no. 3. P. 1638–1648. DOI: 10.25215/1303.151.
31. Patel H., Rehman U., Iqbal F. Evaluating the efficacy of large language models in identifying phishing attempts // *16th International Conference on Human System Interaction (HSI) 2024*. DOI: 10.1109/HSI61632.2024.10613528.
32. Pattinson M., Jerram C., Parsons K., McCormac A. Why do some people manage phishing emails better than others? // *Information Management & Computer Security*. 2012. Vol. 20, no. 1. P. 18–28. DOI: 10.1108/09685221211219173.
33. Sarker O., Haggag S., Jayatilaka A., Liu C. Personalized guidelines for design, implementation and evaluation of anti-phishing interventions // *International Symposium on Empirical Software Engineering and Measurement (ESEM) 2023*. DOI: 10.1109/ESEM56168.2023.10304861.
34. Sheng S., Lanyon M. B., Kumaraguru P., Cranor L. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions // *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010), Atlanta, Georgia, USA, 2010*. Vol. 4. P. 10–15. DOI: 10.1145/1753326.1753383.
35. Sharevski F., Devine A., Pieroni E., Jachim P. Phishing with Malicious QR Codes // *EuroUSEC '22: Proceedings of the 2022 European Symposium on Usable Security*. 2022. P. 160–171. DOI: 10.1145/3549015.3554172.
36. Shonman M., Shi X., Kang M., Wang Z. Using a computational cognitive model to understand phishing classification decisions of email users // *Interacting with Computers*. 2024. Vol. 36, no. 2. P. 113–125. DOI: 10.1093/iwc/iwad054.
37. Spadaro G., Molho C., van Prooijen J. W., Romano A., Mosso C. O., van Lange P. A. M. Corrupt third parties undermine trust and prosocial behaviour between people // *Nature Human Behaviour*. 2023. Vol. 7, no. 1. P. 1–9. DOI: 10.1038/s41562-022-01457-w.
38. Threat Landscape Report 2025: A Year in Review. Версия 1, 8 апреля 2026 г. TLP: CLEAR/PUBLIC. URL: <https://d-russia.ru/wp-content/uploads/2025/09/pdf.pdf>
39. van der Heijden, A., Allodi, L. Cognitive triaging of phishing attacks // *SEC'19: Proceedings of the 28th USENIX Conference on Security Symposium*. P. 1309–1326. DOI: 10.48550/arXiv.1905.02162.

40. Vishwanath, A., Harrison, B., Ng, Y. J. Suspicion, cognition, and automaticity model (SCAM) of phishing susceptibility // *Communication Research*. 2018. Vol. 45, no. 8. P. 1146–1166. DOI: 10.1177/0093650215627483.
41. Wang J., Li Y., Rao H. R. Overconfidence in Phishing Email Detection // *Journal of the Association for Information Systems*. 2021. Vol. 17, no. 11. P. 759–783. DOI: 10.17705/1jais.00442.
42. Zhuo S., Biddle R., Russello G. Lottridge D. Precision Email Simulator for Research on Safety-Critical Phishing Behaviour // *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 2025. No. 1092. P. 1–12.

References

1. Dzhusupova R. A. Vliyaniye moral'nogo i pravovogo soznaniya na social'noe povedenie // *Bulletin of the Academy of Justice*. 2025. DOI: 10.63546/3005-2246.2025.10.2.002. (In Russ.).
2. Landshaft ugroz dlya sistem promyshlennoj avtomatizatsii. Evropa. II kvartal 2025 goda. Available from: <https://ics-cert.kaspersky.ru/publications/reports/2025/09/11/threat-landscape-for-industrial-automation-systems-q2-2025>. (In Russ.).
3. Lobanova E. V. Sociologicheskij analiz vliyaniya korporativnoj kul'tury na effektivnost' obucheniya v tekhnicheskikh universitetah / E. V. Lobanova, G. P. Sapozhnikov // *Modern scientist*. 2024;7: 353–367. (In Russ.).
4. Morosanova V. I. Diagnostika ustojchivosti psihicheskoy samoregulyacii v napryazhennykh usloviyakh v situatsii eksperimenta / V. I. Morosanova, V. N. Krasnikov // *Eksperimental'naya psihologiya*. 2012. Vol. 5;4: 44–53. (In Russ.).
5. Nestik T. A. Social'no-psihologicheskie predposylki i tipy dolgosrochnoj orientatsii: rezul'taty empiricheskogo issledovaniya // *Psihologicheskij zhurnal*. 2021. Vol. 42;4: 28–39. DOI: 10.31857/S020595920016008-4. (In Russ.).
6. Prohorov A. O. Dinamika mental'noj regulyacii psihicheskikh sostoyanij studentov v razlichnykh usloviyakh uchebnoj deyatel'nosti / A. O. Prohorov, A. V. Chernov, M. G. YUsupov // *Eksperimental'naya psihologiya*. 2024. Vol. 17;3: 130–143. DOI: 10.17759/exppsy.2024170309. (In Russ.).
7. Soldatova G. U. Cifrovoe pokolenie Rossii: kompetentnost' i bezopasnost' / G. U. Soldatova, E. I. Rasskazova, T. A. Nestik. M.: Smysl, 2017. 375 s. (In Russ.).
8. Stashkova T. V. Psihologicheskie aspekty modelirovaniya professional'no-lichnostnogo razvitiya pedagoga v sisteme povysheniya kvalifikatsii // *Innovacionnaya nauka psihologiya pedagogika defektologiya*. 2021. Vol. 4;3: 55–64. DOI: 10.23947/2658-7165-2021-4-3-55-64. (In Russ.).
9. Fabrikant M. S. Psihologicheskie faktory kiberbezopasnosti i doverie k lozhnym novostyam v internet-kommunikatsii: obzor sovremennykh zarubezhnykh issledovaniy // *Sovremennaya zarubezhnaya psihologiya*. 2024. Vol. 13;4: 163–171. DOI: 10.17759/jmfp.2024130415. (In Russ.).
10. Abroshan H., Devos J., Poels G., Laermans E. COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic // *IEEE Access*. 2021. Vol. 9. P. 121–130. DOI: 10.1109/ACCESS.2021.3109091.
11. Agagu M., Omorogiuwa O. Investigating and Mitigating User Susceptibility to Phishing Using the Analysis of Demographic Information, Knowledge and Cognitive Experience. *Advances in Multidisciplinary & Scientific // Research Journal Publication*. 2019. Vol. 13, no. 2. P. 94–107. DOI: 10.22624/AIMS/BHI/V11N2P8.
12. Almansoori A., Al-Erman M., Shaalan K. Exploring the frontiers of cybersecurity behavior: A systematic analysis // *Applied Sciences*. 2023. Vol. 13, no. 9. P. 5700. DOI: 10.3390/app13095700.
13. Bitaab M., Cho H., Oest A., Zhang P. Scam pandemic: How attackers exploit public fear through phishing // *Conference: 2020 APWG Symposium on Electronic Crime Research*. DOI: 10.48550/arXiv.2103.12843.
14. Caputo D. D., Pfleeger S. L., Freeman J. D., Johnson M. E. Going spear phishing: Exploring embedded training and awareness // *IEEE Security and Privacy Magazine*. 2014. Vol. 12, no. 1. P. 28–38. DOI: 10.1109/MSP.2013.106.
15. Desolda G., Ferro L. S., Marrella A., Costabile M. F., Catarci T. Human Factors in Phishing Attacks: A Systematic Literature Review // *ACM Computing Surveys (CSUR)*. 2022. Vol. 54, no.8. P. 1–35. DOI: 10.1145/3469886.
16. Diaz A., Sherman A. T., Joshi A. Phishing in an academic community: A study of user susceptibility and behavior // *Cryptologia*. 2019. Vol. 44, no. 1. P. 1–15. DOI: 10.48550/arXiv.1811.06078.
17. Falade P. V. Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks // *International Journal of Scientific Research in Computer Science Engineering and Information Technology*. 2023. Vol. 9, no. 5. P. 185–198. DOI: 10.32628/CSEIT2390533.
18. Fan Z., Li W., Laskey K. B., Chang K. C. Investigation of phishing susceptibility with explainable artificial intelligence // *MDPI*. 2023. Vol. 16, no. 1. DOI: 10.20944/preprints202311.1540.v1.

19. Furnell S., Shah N. J. Home working and cyber security – an outbreak of unpreparedness? // *Computer Fraud & Security*. 2020. no. 8. P. 6–12. DOI: 10.1016/s1361-3723(20)30084-1.
20. Hadlington L. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviours // *Heliyon*. 2017. Vol. 3, no. 7. DOI: 10.1016/j.heliyon.2017.e00346.
21. Jayatilaka A., Arachchilage N. A. G., Babar M. A. Why people still fall for phishing emails: An empirical investigation into how users make email response decisions // *Symposium on Usable Security*. 2024. DOI: 10.14722/usec.2024.23072.
22. Kashapov A., Wu T., Abuadbbba S., Rudolph C. Email summarization to assist users in phishing identification // *Conference: ASIA CCS '22: ACM Asia Conference on Computer and Communications Security*. 2022. DOI: 10.48550/arXiv.2203.13380.
23. Khan N. F., Ikram N., Murtaza H., Javed M. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model // *Computers & Security*. 2022. Vol. 125. P. 7–8. DOI: 10.1016/j.cose.2022.103049.
24. Korteling J. E., Paradies G. L., Sassen-van Meer J. P. Cognitive bias and how to improve sustainable decision making // *Front. Psychol., Sec. Cognitive Science*. 2023. Vol.14. DOI: 10.3389/fpsyg.2023.1129835.
25. Kumaraguru P., Sheng S., Acquisti A., Cranor L. Teaching Johnny not to fall for phish // *ACM Transactions on Internet Technology*. 2010. Vol. 10, no. 2. DOI: 10.1145/1754393.1754396.
26. Malloy T., Ferreira M. J., Fang F., Gonzalez C. Leveraging a cognitive model to measure subjective similarity of human and GPT-4 written content // *Conference: Proceedings of the 28th Conference on Computational Natural Language Learning*. 2024. DOI: 10.48550/arXiv.2409.00269.
27. Marin I. A., Burda P., Zannone N., Allodi L. The influence of human factors on the intention to report phishing emails // *Conference: CHI '23: CHI Conference on Human Factors in Computing Systems*. 2023. No. 20. P. 1–18. DOI: 10.1145/3544548.3580985.
28. Morrow E. Scamming higher ed: An analysis of phishing content and trends // *Computers in Human Behavior*. 2024. Vol. 158, no. 3. DOI: 10.1016/j.chb.2024.108274.
29. Mousa J. An overview of phishing victimization: Human factors, training and the role of emotions // *Computer Science & Information Technology*. 2022. Vol. 12, no. 13. P. 197–207. DOI: 10.5121/csit.2022.121319.
30. Nagar P. The Psychology of Cyber Fraud: Unraveling the Tactics Behind Modern-Day Scams // *The International Journal of Indian Psychology*. 2025. Vol. 13, no. 3. P. 1638–1648. DOI: 10.25215/1303.151.
31. Patel H., Rehman U., Iqbal F. Evaluating the efficacy of large language models in identifying phishing attempts // *16th International Conference on Human System Interaction (HSI) 2024*. DOI: 10.1109/HSI61632.2024.10613528.
32. Pattinson M., Jerram C., Parsons K., McCormac A. Why do some people manage phishing emails better than others? // *Information Management & Computer Security*. 2012. Vol. 20, no. 1. P.18-28. DOI: 10.1108/09685221211219173.
33. Sarker O., Haggag S., Jayatilaka A., Liu C. Personalized guidelines for design, implementation and evaluation of anti-phishing interventions // *International Symposium on Empirical Software Engineering and Measurement (ESEM) 2023*. DOI: 10.1109/ESEM56168.2023.10304861.
34. Sheng S., Lanyon M. B., Kumaraguru P., Cranor L. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions // *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010)*, Atlanta, Georgia, USA, 2010. Vol. 4. P. 10–15. DOI: 10.1145/1753326.1753383.
35. Sharevski F., Devine A., Pieroni E., Jachim P. Phishing with Malicious QR Codes // *EuroUSEC '22: Proceedings of the 2022 European Symposium on Usable Security*. 2022. P. 160–171. DOI: 10.1145/3549015.3554172.
36. Shonman M., Shi X., Kang M., Wang Z. Using a computational cognitive model to understand phishing classification decisions of email users // *Interacting with Computers*. 2024. Vol. 36, no. 2. P. 113–125. DOI: 10.1093/iwc/iwad054.
37. Spadaro G., Molho C., van Prooijen J. W., Romano A., Mosso C. O., van Lange P. A. M. Corrupt third parties undermine trust and prosocial behaviour between people // *Nature Human Behaviour*. 2023. Vol. 7, no. 1. P. 1–9. DOI: 10.1038/s41562-022-01457-w.
38. Threat Landscape Report 2025: A Year in Review. Версия 1, 8 апреля 2026 г. TLP:CLEAR/PUBLIC. URL: <https://d-russia.ru/wp-content/uploads/2025/09/pdf.pdf>
39. van der Heijden, A., Allodi, L. Cognitive triaging of phishing attacks // *SEC'19: Proceedings of the 28th USENIX Conference on Security Symposium*. P. 1309–1326. DOI: 10.48550/arXiv.1905.02162.
40. Vishwanath, A., Harrison, B., Ng, Y. J. Suspicion, cognition, and automaticity model (SCAM) of phishing susceptibility // *Communication Research*. 2018. Vol. 45, no. 8. P. 1146–1166. DOI: 10.1177/0093650215627483.

41. Wang J., Li Y., Rao H. R. Overconfidence in Phishing Email Detection // Journal of the Association for Information Systems. 2021. Vol. 17, no. 11. P. 759–783. DOI: 10.17705/1jais.00442.
42. Zhuo S., Biddle R., Russello G. Lottridge D. Precision Email Simulator for Research on Safety-Critical Phishing Behaviour // CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. 2025. No. 1092. P. 1–12.

Информация об авторах

Е. П. Солдатова – доктор психологических наук, профессор

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 20.03.2026;
одобрена после рецензирования 17.08.2026;
принята к публикации 28.09.2026.

Information about the authors

E. P. Soldatova – Doctor of Sciences (Pedagogy), Professor

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

The article was submitted 20.03.2026;
approved after reviewing 17.08.2026;
accepted for publication 28.09.2026.