

УДК 331.08

DOI 10.22213/2618-9763-2026-3-36-43

А. И. Троянская, кандидат психологических наук, доцент

Ю. В. Тихонова, магистрант

Ижевский государственный технический университет имени М. Т. Калашникова, Ижевск, Россия

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В статье рассматривается актуальная и масштабная проблема исследования роли человеческого фактора в обеспечении информационной безопасности, с которой сталкивается практически каждый человек и предприятие. Подчеркивается стратегическое значение решения этой проблемы на предприятиях оборонно-промышленного комплекса. Отмечается, что тема не является методологически разработанной в современной научной литературе, наблюдается недостаток статистически подкрепленных исследований информационной безопасности. Приводятся контуры и хронология развертывания типичных угроз, с которыми сталкивается предприятие оборонно-промышленного комплекса: фишинг и целевая социальная инженерия, нарушение регламентов работы с конфиденциальной информацией, использование неразрешенных устройств и носителей. Дана статистика причин инцидентов и их последствий. Проведена оценка уязвимых категорий персонала предприятия, спрогнозирован возможный уровень ущерба при разных типах инцидентов. Представлены программы мероприятий для коррекции влияния человеческого фактора на информационную безопасность. Программы дифференцированы для разных возрастных категорий персонала. Они предполагают формирование проактивной культуры безопасности, повышение вовлеченности и развитие метакогнитивных навыков для молодых сотрудников, а также управление психоэмоциональной нагрузкой, адаптацию к индивидуальным когнитивным профилям, формирование психологической устойчивости к манипуляциям для более старших сотрудников. Программы учитывают социальный (должностная категория) и мотивационный (снижение нагрузки, формирование лояльности, сочетание контроля и вознаграждения) аспекты. Сделан вывод о заинтересованности менеджмента в проведении научных исследований в области повышения информационной безопасности предприятия с учетом влияния человеческого фактора, а также в разработке и внедрении программ коррекции его влияния, поскольку потенциальные угрозы во много раз превышают предполагаемые затраты на профилактические мероприятия.

Ключевые слова: информационная безопасность; человеческий фактор; цифровая экономика; защита данных; культура безопасности

Введение

Проблема исследования состоит в том, что в современной цифровой экономике, характеризующейся повсеместной цифровизацией бизнес-процессов и ростом сложности ИТ-инфраструктур, сохраняется противоречие: несмотря на развитие технологических средств защиты информации – от искусственного интеллекта до многофакторной аутентификации, человеческий фактор остается одним из наиболее уязвимых и непредсказуемых мест в системе безопасности предприятий. Многообразие возможных человеческих ошибок создает предпосылки для появления практически всех потенциальных угроз информационной безопасности: от искажения информации до невозможности ее использования.

Выстраивая архитектуру безопасности предприятия, первостепенное внимание принято уделять техническим инструментам, но их защиту легко можно обойти, если сотрудники сами предоставляют доступ к информации. Только с помощью технических средств без учета человеческого фактора невозможно обеспечить

полноценную работу системы информационной безопасности предприятия [1].

В теоретическом плане проблема информационной безопасности не принадлежит к числу фундаментально разработанных научных направлений [2].

Были проведены исследования поведенческих аспектов защиты, выявляющие роль когнитивных искажений в возникновении угроз (Б. Шнайер); изданы работы по психологии фишинга и социальной инженерии, анализирующие технические и психологические вопросы (М. Якобссон, С. Майерс) [3].

Российские исследователи информационной безопасности отмечают роль человеческого фактора в управлении рисками, анализируют вопросы безопасности при работе с системами искусственного интеллекта (А. Лукацкий [4]). Сотрудниками лаборатории открытых информационных технологий факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова разработаны методики оценки навыков

кибербезопасности персонала (О. С. Белякова, В. А. Сухомлин [5]). Отдельные направления занимаются коррекцией человеческих рисков в Лаборатории Касперского, например, направление *secure by design* (А. Ярных [6]). Отдельно необходимо отметить, что тема человеческого фактора в информационной безопасности привлекает внимание молодых исследователей М. А. Лебедев, Д. А. Демкин, А. В. Ванин, А. В. Марченко [7].

Источниками данных по промышленному сектору являются регулярные публичные отчеты Федеральной службы по техническому и экспортному контролю («Обзор основных угроз информационной безопасности»), отчет *Positive Technologies*, часть ежегодного *Security Bulletin Kaspersky ICS CERT*¹.

Информационная безопасность в документах Федеральной службы по техническому и экспортному контролю (ФСТЭК) России определяется как комплекс мер, направленных на защиту информации от угроз, несанкционированного доступа, утечек по техническим каналам, а также на обеспечение целостности, конфиденциальности и доступности данных в информационных системах.

Человеческий фактор может быть рассмотрен в двух значимых смысловых аспектах: 1 – как вся совокупность качественных характеристик, особенностей и свойств персонала и 2 – как причина ошибочных действий персонала [8]. Характеристики человека могут не соответствовать уровню сложности задач деятельности. Тогда люди совершают ошибки непреднамеренно, выполняют ошибочные действия, считая их подходящими.

Человеческий фактор может быть применим и оказывать воздействие на сферу информационной безопасности. Человеческий фактор в информационной безопасности – это совокупность психологических, поведенческих и социальных характеристик людей, которые могут влиять на безопасность информационных систем и данных. К таким факторам относятся ошибки, неосторожность, недостаток знаний и навыков в области информационной безопасности, недостаток мотивации, неграмотное использование технологий, когнитивные искажения [9].

Целью исследования является установление особенностей человеческого влияния в сфере информационной безопасности, создание ряда мероприятий, регулирующих это влияние для повышения уровня информационной безопасности на предприятиях оборонно-промышленного комплекса.

Исследование роли человеческого фактора в информационной безопасности предприятия

Промышленный сектор является объектом повышенного внимания со стороны злоумышленников и киберпреступников. Случайная человеческая ошибка в последние годы стала причиной большего количества происшествий (32 %), чем любой другой фактор [10]. Распределение причин инцидентов, связанных с человеческим фактором, в области информационной безопасности по предприятиям оборонно-промышленного комплекса приведено в табл. 1.

Таблица 1. Статистика инцидентов в области информационной безопасности в связи с человеческим фактором на предприятиях ОПК (за 2022–2024 гг.)

Table 1. Statistics of information security incidents related to the human factor at defense industry enterprises (for 2022–2024)

Тип ошибки/инцидента	Доля от общего числа инцидентов, %	Характерные последствия
Фишинг и целевая социальная инженерия	32	Утечка учетных данных, заражение вредоносным программным обеспечением (ПО)
Нарушение регламентов работы с конфиденциальной информацией	25	Несанкционированное распространение данных
Использование неразрешенных устройств и носителей	18	Заражение сетей, утечки через съемные носители
Ненадлежащая настройка систем защиты	12	Создание уязвимостей в корпоративной инфраструктуре
Слабые пароли и нарушение парольной политики	8	Несанкционированный доступ к системам
Несвоевременное обновление ПО	5	Эксплуатация известных уязвимостей

Источник: составлена авторами.

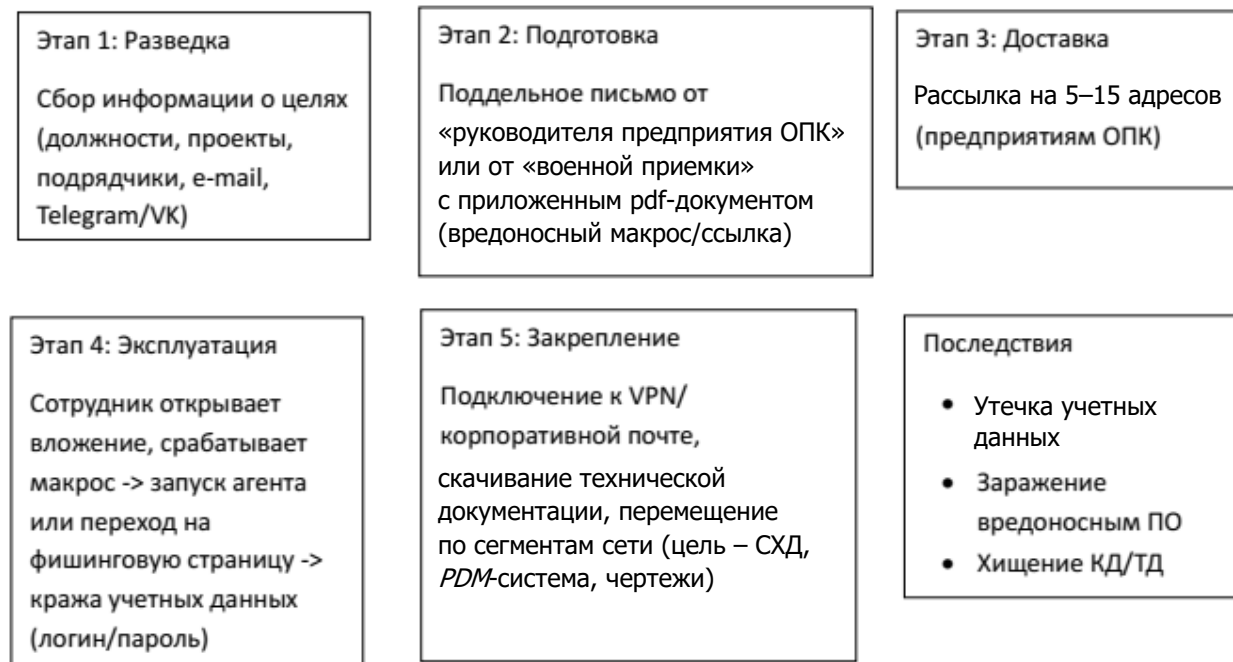
¹ Кибербезопасность промышленных предприятий // URL: <https://lp.kaspersky.com/global/ksb2025-ics-cert-trends-and-predictions/> (дата обращения: 16.08.2026).

Рассмотрев данные, необходимо отметить, что в настоящее время применяемые меры противодействия проблеме не являются достаточными, и вопрос остается актуальным.

Важным этапом исследования является анализ возможных сценариев реализации инцидентов информационной безопасности. Их схематическое представление позволяет структурировать основные этапы развития угроз, выявить

ключевые точки уязвимости и конкретизировать роль человеческого фактора в возникновении инцидентов (рис. 1–3).

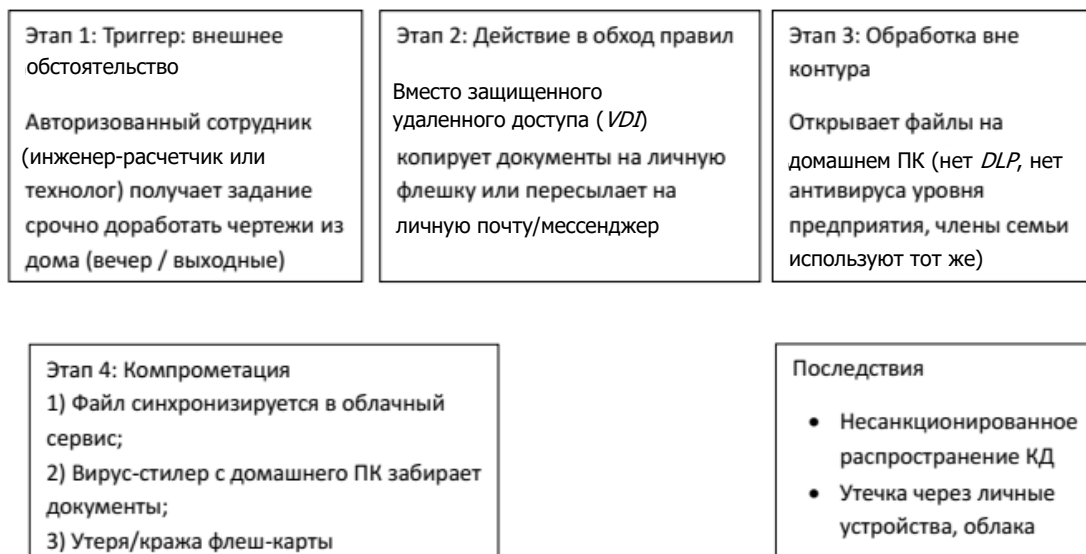
Наиболее актуальные сценарии инцидентов: 1 – фишинг и целевая социальная инженерия; 2 – нарушение регламентов работы с конфиденциальной информацией; 3 – использование неразрешенных устройств и носителей.



Источник: выполнен авторами.

Рис. 1. Примерные этапы инцидента «фишинг и целевая социальная инженерия»

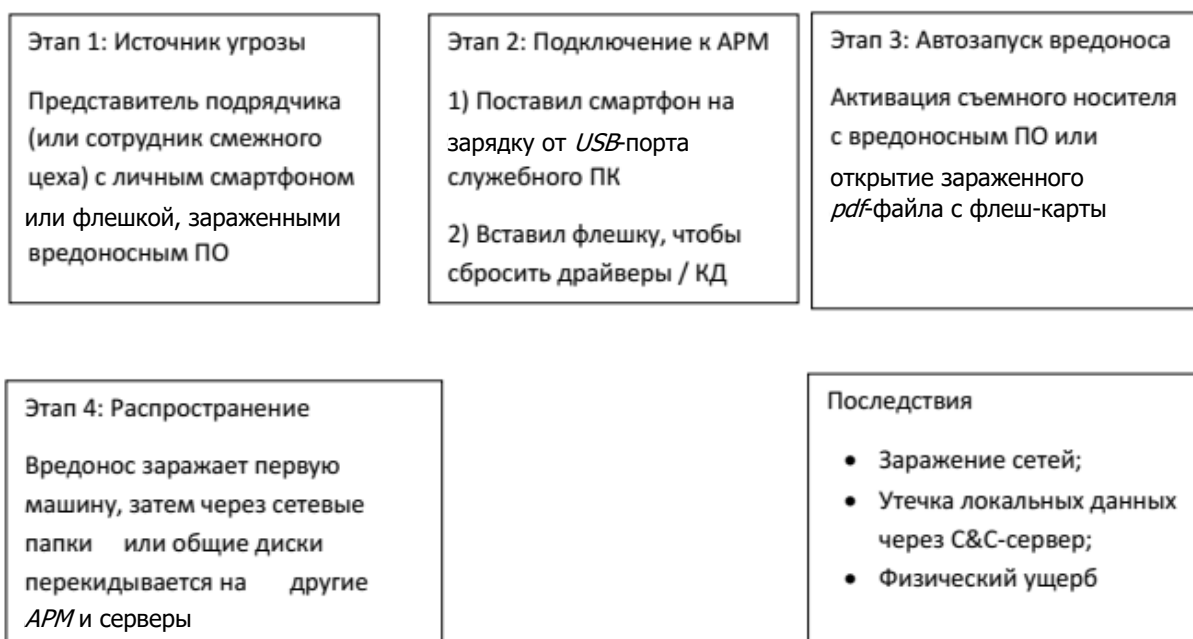
Fig. 1. Approximate stages of the “phishing and targeted social engineering” incident



Источник: выполнен авторами.

Рис. 2. Примерные этапы инцидента «Нарушение регламентов работы с конфиденциальной информацией»

Fig. 2. Approximate stages of the incident “Violation of regulations for handling confidential information”



Источник: выполнен авторами.

Рис. 3. Примерные этапы инцидента «Использование неразрешенных устройств и носителей»

Fig. 3. Approximate stages of the incident "Use of unauthorized devices and media"

Для более детального понимания специфики рассматриваемой проблемы необходимо проанализировать данные, характеризующие частоту попыток реализации основных инцидентов информационной безопасности (табл. 2). Такой подход позволяет конкретизировать ранее выделенные угрозы и оценить их проявление в исследуемом периоде.

В табл. 2 представлена оценка количества попыток реализации основных инцидентов информационной безопасности на одном предприятии ОПК в 2022–2024 гг. Следует отметить, что приведенные значения носят усредненный характер, используются в целях аналитического обобщения и не являются конфиденциальными показателями внутренней отчетности.

Таблица 2. Оценка количества попыток реализации основных инцидентов информационной безопасности на предприятии в 2022–2024 гг., ед.

Table 2. Assessment of the number of attempts to implement major information security incidents at the enterprise in 2022–2024, cases

Вид инцидента	Годы		
	2022	2023	2024
Фишинговые атаки	10	16	22
Инциденты вследствие ошибок персонала	7	10	12
Компрометация учетных данных	5	8	11
Использование несанкционированных носителей и ПО	3	5	7
Нарушения регламентов ИБ	4	6	9

Примечание: представлены усредненные данные, используемые в аналитических целях.

Источник: составлена авторами.

Как видно из табл. 2, наиболее заметный рост в исследуемом периоде наблюдается по фишинговым атакам и инцидентам, связанным с компрометацией учетных данных, что подтверждает усиление рисков, обусловленных человеческим фактором.

Для более детального рассмотрения влияния человеческого фактора на уровень информаци-

онной безопасности (ИБ) целесообразно обратиться к характеристике наиболее уязвимых категорий персонала, уровню их подготовки в области информационной безопасности и возможным финансовым последствиям реализации инцидентов (табл. 3).

Таблица 3. Оценка уязвимых категорий персонала, уровня подготовки в области информационной безопасности и возможного финансового ущерба

Table 3. Assessment of vulnerable categories of personnel, level of training in the field of information security and possible financial damage

Категория сотрудников	Возрастная группа	Пол	Наиболее вероятный вид угрозы	Доля сотрудников, прошедших обучение по ИБ, %	Возможные последствия	Примерный финансовый ущерб при инциденте, тыс. руб.
Административный персонал	25–40 лет	Смешанный состав	Фишинг, компрометация корпоративной почты	55	Утрата доступа к учетным записям, утечка служебной информации	120–200
Бухгалтерия и финансовые службы	30–50 лет	Преимущественно женщины	Фишинг, подмена реквизитов, вредоносные вложения	60	Ошибочные платежи, компрометация финансовой документации	250–500
Руководящий состав	35–60 лет	Смешанный состав	Целевой фишинг, социальная инженерия	45	Утечка конфиденциальной информации, репутационные потери	300–600
IT-специалисты	25–45 лет	Преимущественно мужчины	Ошибки конфигурации, нарушение правил доступа	80	Нарушение доступности сервисов, технические сбои	200–400
Новые сотрудники	22–30 лет	Смешанный состав	Фишинг, ошибки при обработке данных	35	Локальные утечки информации, нарушение внутренних регламентов	80–150

Примечание: представлены усредненные данные; показатели финансового ущерба носят оценочный характер и приведены в аналитических целях.

Источник: составлена авторами.

Представленные данные позволяют сделать вывод о том, что наибольшие финансовые последствия связаны с инцидентами, затрагивающими бухгалтерские подразделения и руководящий состав. В то же время недостаточный уровень охвата обучения по информационной безопасности в ряде категорий персонала создает дополнительные условия для реализации угроз, обусловленных человеческим фактором.

Анализ результатов

Таким образом, для изменения статистики по инцидентам в лучшую сторону предлагается ввести ряд мероприятий: регулярное обучение, а именно целевые тренинги на инциденты, специализированные курсы по информационной безопасности, повышение квалификации в вопросах безопасности, формирование культуры безопасности, а именно закрепление норм в корпоративных кодексах, регулярные тематические брифинги, повышение осведомленности

через средства визуализации, дополнительные технические инструменты на отдельных участках, например, автоматизация контроля доступа.

Мероприятия необходимо специфицировать для разных возрастных категорий персонала, условно обозначенных как «молодые» и «старшие» сотрудники.

Для «молодых» сотрудников актуально формирование проактивной культуры безопасности. Необходимо создать внутреннюю мотивацию через понимание личной ответственности. Если сотрудник понимает, почему вопросы безопасности критически важны, его действия становятся осознанными, а не автоматическими. Ученые стараются создавать теоретические модели в области кибер-этики. Например, Р. Мэйсон с соавторами выделяет следующие аспекты кибер-этичного поведения: доступность, точность, личная свобода и собственность [11]. Человек перестает быть пассивным исполнителем и превращается в активного защитника. Таким обра-

зом, возможно снижение числа нарушений по невнимательности на 40–60 %.

Укрепление лояльности через вовлеченность относится к мерам психологического воздействия, которые можно реализовать с помощью геймификации обучения, системы поощрений за соблюдение стандартов, поддержание открытого диалога о рисках. Это демонстрирует заботу организации о своем персонале. Сотрудники начинают воспринимать требования информационной безопасности не как ограничение их свободы, а как инструмент их собственной защищенности. Результатом может стать увеличение приверженности организации на 35–50 % (по шкале *Organizational Commitment Questionnaire (OCQ)* [12].

Развитие метакогнитивных навыков уместно для «молодых» сотрудников с целью преодоления влияния когнитивных искажений

Люди с недостаточно высоким уровнем знаний или навыков в какой-либо области склонны переоценивать собственную компетентность, не всегда осознают свои ошибки. Этот феномен получил название эффекта Даннинга – Крюгера. И наоборот, высококвалифицированные люди часто недооценивают свои знания, полагая, что задачи, которые им кажутся легкими, будут легкими и для других. Одно из возможных решений: проведение в рамках плана обучения тренингов по критическому мышлению и саморефлексии. Сотрудники начинают осознавать действие таких когнитивных искажений, как эффект избыточной уверенности («со мной этого не случится») или гиперболическое обесценивание (когда переоцениваются срочные, но менее важные задачи, в ущерб долгосрочным). В качестве результата можно предположить на 45 % меньше решений, принятых под влиянием эмоциональных триггеров.

Для «старших» сотрудников целесообразны меры по регуляции психоэмоциональной нагрузки, проектирование инструкций действий в случае инцидента. Постоянное психологическое напряжение приводит к перегрузке, что, в свою очередь, увеличивает вероятность ошибочных действий. Внедрение четких, понятных алгоритмов поведения в нештатных ситуациях значительно снижает эту нагрузку. Сотрудник перестает действовать в условиях неопределенности и паники, четко знает, к кому обратиться. Возможный результат – снижение на 25–30 % ошибок, вызванных паникой при инцидентах.

Возможна адаптация тренингов к индивидуальным когнитивным профилям. Перспектив-

ны исследования влияния типологических особенностей человека, свойств темперамента на поведение в ситуациях, значимых для поддержания информационной безопасности. Эффективным представляется разработка персонализированных инструкций и тренингов, учитывающих особенности темперамента, когнитивного стиля и скорости обработки информации сотрудников. В перспективе ожидается сокращение времени реакции на угрозы в два раза.

Формирование устойчивости, «психологического иммунитета» к манипуляциям путем регулярного моделирования реальных сценариев фишинга, вишинга и других методов социальной инженерии. В безопасной учебной среде у сотрудника формируется способность распознавать манипулятивные приемы. Желаемым результатом будет пресечение 90 % попыток внешнего воздействия на персонал [13].

Выводы

Представленные вариативные программы управления влиянием человеческого фактора на информационную безопасность предприятия перспективны для внедрения. Управленческий персонал заинтересован в разработке таких программ, в проведении научных исследований в данной области, поскольку потенциальные угрозы во много раз превышают предполагаемые затраты на профилактические мероприятия.

В качестве перспектив исследования запланировано изучение роли психофизиологических особенностей персонала, типологических свойств темперамента в процессе обеспечения информационной безопасности.

Очень высокую значимость приобрела задача осознанного внедрения технологических решений. Применяемые технологии существенно влияют на социальные процессы и взаимодействие [14]. Недопустимо отдавать приоритет исключительно техническим аспектам и совершенствованию программного обеспечения, необходимо развивать коммуникационные стратегии внедрения технических решений, целенаправленно формировать профессиональные навыки и ценности людей, их применяющих.

Библиографические ссылки

1. Schneier B. The Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back. New York: W.W. Norton & Company. 2023. 304 p.
2. Солдатова Г. У., Войскунский А. Е. Социально-когнитивная концепция цифровой социализации: новая экосистема и социальная эволюция психики // Психология. Журнал Высшей школы экономики.

2021. Т. 18. № 3. С. 431–450. DOI: 10.17323/1813-8918-2021-3-431-450. EDN: RSSHPN

3. Ванин А. В., Марченко А. В. Человеческий фактор в информационной безопасности организации: направления исследований, меры противодействия, перспективы изучения // Политехнический молодежный журнал. 2020. № 04 (45). С. 2. DOI: 10.18698/2541-8009-2020-4-601. EDN: NTXMLM

4. Лукацкий А. Расходы на кибербезопасность. URL: <https://lukatsky.ru/threats/model-ugroz-ii-ot-sbera-i-da-i-net.html> (дата обращения: 06.09.2026).

5. Белякова О. С., Сухомлин В. А. Исследование навыков кибербезопасности стандарта SFIA8 // International Journal of Open Information Technologies. 2022. Vol. 10. No. 7. С. 156–163.

6. Ярных А. Самая большая опасность – это ощущение безопасности // ГИТР. URL: <https://gitr.ru/news/andrey-yarnyh> (дата обращения: 12.05.2026).

7. Ванин А. В., Марченко А. В. Человеческий фактор в информационной безопасности организации: направления исследований, меры противодействия, перспективы изучения // Политехнический молодежный журнал. 2020. № 04 (45). С. 2. DOI: 10.18698/2541-8009-2020-4-601. EDN: NTXMLM

8. Троянская А. И., Прасолов М. И. Роль человеческого фактора в системе управления персоналом в условиях цифровой трансформации // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32. № 1. С. 88–94. DOI: 10.35634/2412-9593-2022-32-1-88-94. EDN: QCFUXW

9. Самарская Н. А. Влияние человеческого фактора на трансформацию охраны труда в контексте современной теории поколений // Лидерство и менеджмент. 2023. Т. 10. № 3. С. 837–856. DOI: 10.18334/lim.10.3.118237. EDN: UDSUKO

10. Киберугрозы для промышленных предприятий и ОТ-инфраструктур в 2024 году // Security Bulletin 2023. URL: <https://securelist.ru/ksb-ics-predictions-2024/108436/> (дата обращения: 06.09.2026).

11. Воробьева К. И., Долгачев М. В., Заславский Д. А. Психологические ресурсы кибербезопасности человека // Социальные и гуманитарные науки на Дальнем Востоке. 2020. Т. XVII. Вып. 4. С. 150–157. DOI: 10.31079/1992-2868-2020-17-4-150-157. EDN: SGXSQA

12. Потапова Ю. В., Климухина В. А. Структура и факторы формирования организационной приверженности: теоретическая модель // Организационная психология. 2024. Т. 14. № 3. С. 117–146. DOI: 10.17323/2312-5942-2024-14-3-117-146. EDN: KVVYBFW

13. Blinnikova I., Matyushin V. Regulation and experience of emotions as predictors of burnout syndrome in mental health specialists // European Psychiatry. Cambridge University Press. 2020. Vol. 63. No. S1, P. 156. DOI: 10.1192/j.eurpsy.2020.5

14. Цифровая трансформация процессов повышения квалификации персонала АО «Омутнинский металлургический завод» / О. Б. Главатских, А. И. Троянская, М. И. Прасолов, Е. В. Царева // Глобальный научный потенциал. 2021. № 1 (118). С. 109–111. EDN: UAIMNQ

References

1. Schneier B. The Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back. New York, W.W. Norton & Company, 2023, 304 p. (in Engl.).

2. Soldatova G.U., Voiskunskii A.E. [Sotsial'nokognitivnaya kontseptsiya tsifrovoy sotsializatsii: novaya ehkositema i sotsial'naya ehvolyutsiya psikhiki]. *Psikhologiya. Zhurnal Vysshei Shkoly ehkonomiki. Natsional'nyi issledovatel'skii universitet "Vysshaya shkola ehkonomiki"*, 2021, vol. 18, no. 3, pp. 431-450. (in Russ.). DOI: 10.17323/1813-8918-2021-3-431-450. EDN: RSSHPN

3. Vanin A.V., Marchenko A.V. [Chelovecheskii faktor v informatsionnoi bezopasnosti organizatsii: napravleniya issledovaniy, mery protivodeistviya, perspektivy izucheniya]. *Politekhnicheskii molodezhnyi zhurnal*, 2020, no. 04 (45), p. 2. (in Russ.). DOI: 10.18698/2541-8009-2020-4-601. EDN: NTXMLM

4. Lukatskii A. *Raskhody na kiberbezopasnost'* [Cybersecurity costs]. (in Russ.). Available at: <https://www.securitylab.ru/analytics/> (accessed 06.09.2026).

5. Belyakova O.S., Sukhomlin V.A. [Issledovanie navykov kiberbezopasnosti standarta SFIA8] *International Journal of Open Information Technologies*, 2022, vol. 10, no. 7, pp. 156-163. (in Russ.).

6. Yarnykh A. *Samaya bol'shaya opasnost' – ehto oshchushchenie bezopasnosti* [The biggest danger is the feeling of security]. Available at: <https://gitr.ru/news/andrey-yarnyh>. (accessed 12.05.2026).

7. Vanin A.V., Marchenko A.V. [Chelovecheskii faktor v informatsionnoi bezopasnosti organizatsii: napravleniya issledovaniy, mery protivodeistviya, perspektivy izucheniya]. *Politekhnicheskii molodezhnyi zhurnal*, 2020, no. 04 (45), p. 2. (in Russ.). DOI: 10.18698/2541-8009-2020-4-601. EDN: NTXMLM

8. Troyanskaya A.I., Prasolov M.I. [Rol' chelovecheskogo faktora v sisteme upravleniya personalom v usloviyakh tsifrovoy transformatsii]. *Vestnik Udmurtskogo universiteta. Seriya Ehkonomika i pravo*, 2022, vol. 32, no. 1, pp. 88-94. (in Russ.). DOI: 10.35634/2412-9593-2022-32-1-88-94. EDN: QCFUXW

9. Samarskaya N.A. [Vliyanie chelovecheskogo faktora na transformatsiyu okhrany truda v kontekste sovremennoi teorii pokolenii]. *Liderstvo i menedzhment*, 2023, vol. 10, no. 3, pp. 837–856. (in Russ.). DOI: 10.18334/lim.10.3.118237. EDN: UDSUKO

10. *Kiberugrozy dlja promyshlennykh predpriyatij i OT-infrastruktur v 2024 godu* [Cyber threats to industrial enterprises and OT infrastructures in 2024]. *Security Bulletin* 2023. (in Russ.). Available at: <https://securelist.ru/ksb-ics-predictions-2024/108436/> (accessed 06.09.2026).

11. Vorob'eva K.I., Dolgachev M.V., Zaslavskii D.A. [Psikhologicheskie resursy kiberbezopasnosti cheloveka]. *Sotsial'nye i gumanitarnye nauki na Dal'nem Vostoke*, 2020, vol. XVII, no. 4, pp. 150-157. (in Russ.). DOI: 10.31079/1992-2868-2020-17-4-150-157. EDN: SGXSQA

12. Potapova Yu.V., Klimukhina V.A. [Struktura i faktory formirovaniya organizatsionnoi priverzhennosti: teoreticheskaya model'.] *Organizatsionnaya psikhologiya*, 2024, vol. 14, no. 3, pp. 117-146. (in Russ.). DOI: 10.17323/2312-5942-2024-14-3-117-146. EDN: KVYBFW

13. Blinnikova I., Matyushin V. Regulation and experience of emotions as predictors of burnout syndrome

in mental health specialists. *European Psychiatry*. Cambridge University Press, 2020, vol. 63, no. S1, p. 156. DOI: 10.1192/j.eurpsy.2020.5

14. Glavatskikh O.B., Troyanskaya A.I., Prasolov M.I., Tsareva E.V. [Tsifrovaya transformatsiya protsessov povysheniya kvalifikatsii personala AO "Omutninskii metallurgicheskii zavod"]. *Global'nyi nauchnyi potentsial*, 2021, no. 1 (118), pp. 109-111. (in Russ.). EDN: UAIMNQ

A. I. Troyanskaya, PhD in Psychology, Associate Professor
Yu. V. Tikhonova, Master's Degree Student
Kalashnikov Izhevsk State Technical University, Izhevsk, Russia

THE HUMAN FACTOR IN ENSURING THE INFORMATION SECURITY OF THE ENTERPRISE

The article discusses the urgent and large-scale problem of studying the role of the human factor in ensuring information security, which is faced by almost every person and enterprise. The strategic importance of solving this problem at the enterprises of the defence-industrial complex is emphasized. It is noted that the topic is not methodologically developed in modern scientific literature, and there is a lack of statistically supported information security studies. This article provides the outlines and chronology of the deployment of typical threats faced by enterprises of the military-industrial complex: phishing and targeted social engineering, violation of regulations for working with confidential information, the use of unauthorized devices and media. Statistics on the causes of incidents and their consequences are given. An assessment of vulnerable categories of the company's personnel was carried out, and the possible level of damage in different types of incidents was predicted. The program of measures for correcting the influence of the human factor on information security is presented. The programs are differentiated for different age categories of staff. They involve the formation of a proactive safety culture, increased engagement, and the development of metacognitive skills for young employees. As well as psychoemotional stress management, adaptation to individual cognitive profiles, and the formation of psychological resistance to manipulation for more senior employees. The programs take into account social (job category) and motivational (load reduction, loyalty formation, a combination of control and remuneration) aspects. It is concluded that management is interested in conducting scientific research in the field of improving the information security of an enterprise, taking into account the influence of the human factor, as well as in developing and implementing programs to correct its impact, since potential threats are many times higher than the estimated costs of preventive measures.

Keywords: information security; human factor; digital economy; data protection; security culture

Получена: 19.06.2026
ГРНТИ 81.93.29

Образец цитирования

Троянская А. И., Тихонова Ю. В. Человеческий фактор в обеспечении информационной безопасности предприятия // Социально-экономическое управление: теория и практика. 2026. Т. 21, № 3. С. 36–43. DOI: 10.22213/2618-9763-2026-3-36-43

For Citation

Troyanskaya A.I., Tikhonova Yu.V. [The human factor in ensuring the information security of the enterprise]. *Social'no-ekonomicheskoe upravlenie: teoria i praktika*, 2026, vol. 21, no. 3, pp. 36-43 (in Russ.). DOI: 10.22213/2618-9763-2026-3-36-43