РОЛЬ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В ВОЗНИКНОВЕНИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена проблемам обеспечения информационной безопасности с позиции влияния и управления человеческим фактором. Анализируется влияние ошибок, невнимательности и недостаточной осведомленности сотрудников на уровень безопасности организаций. Рассматриваются индивидуальные и организационные факторы, способствующие инцидентам информационной безопасности. Основное внимание уделяется необходимости осознания серьезности проблемы человеческого фактора и разработке подходов для минимизации рисков, связанных с ошибками и умышленными действиями.

Ключевые слова: человеческий фактор, информационная безопасность, утечка информации, кибератаки, ошибки сотрудников, организационные факторы, индивидуальные факторы.

Угроза человеческого фактора для информационной безопасности существовала всегда, но в современном мире, где утечки информации демонстрируют свой непрерывный рост, а кибератаки на организации становятся все более сложными и изощренными, приводя ко все более тяжелым последствиям, человеческий фактор становится ключевым элементом, определяющим уровень информационной безопасности организаций. Более того, ошибки, невнимательность, умышленные действия сотрудников, их недостаточная осведомленность о современных методах кибератак, подверженность социальному инжинирингу делают организации невероятно уязвимыми перед угрозой утечки (утери) конфиденциальной информации.

Ученые неоднократно поднимали вопрос о проблеме человеческого фактора, но наиболее полно раскрыл ее и показал возможные катастрофические последствия нобелевский лауреат, израильско-американский психолог Д. Канеман в книге «Шум. Несовершенство человеческих суждений» [Канеман и др., с. 521]. Однако до сих пор никто не предложил конкретных подходов или инструментов, которые могли бы помочь экспертам и бизнесу в решении этой проблемы.

На протяжении многих лет специалисты по информационной безопасности принимали как данность превосходство технологий над человеческим фактором. Но современная практика в сфере безопасности показывает, что без решения проблемы человеческого фактора технологические решения не могут обеспечить надежную защиту различных структур.

¹ Научный руководитель: К. А. Уланов, канд. ист. наук, доцент УрФУ.

Этот общий вывод стал результатом серии отчетов, инициированных как государственными органами, так и ведущими организациями по кибербезопасности, финансовыми учреждениями, а также аналитическими и экспертными компаниями.

Согласно данным этих исследований и отчетов, человеческий фактор остается основным источником нарушений безопасности, составляя до 95 % всех инцидентов [Отчет о глобальных рисках..., с. 45]. В 2022 г. 82 % зарегистрированных кибератак были связаны с действиями людей [Отчет MIT Sloan, с. 8], а количество инсайдерских угроз увеличилось на 44 % [Отчет Ponemon Intsitute, с. 31]. Средняя стоимость утечки данных составляет 4,24 млн долларов [Отчет о глобальных рисках..., с. 45]. Российские компании, такие как «РТК-Солар» [Отчет Ростелеком-Солар, с. 6] и ГК InfoWatch [Отчет ГК InfoWatch, с. 9], подтверждают эти тенденции, указывая, что более половины инцидентов связаны с внутренними нарушителями, включая как непреднамеренные, так и умышленные утечки информации. Основным выводом заключается в необходимости решения главной проблемы в области информационной безопасности – человеческого фактора. Так что первое обязательное условие движения в сторону более высокой защищенности заключается в осознании серьезности вопроса.

Ошибки пользователей, недостаток осведомленности сотрудников об угрозах являются основными факторами, способствующими инцидентам в области информационной безопасности.

Часто такие ошибки происходят из-за невнимательности, невежества или недостатка знаний в области информационной безопасности. Для описания подобных явлений ученые ввели термин «человеческий фактор», который первоначально использовался в научно-технической сфере [Самарская, с. 837–856]. Со временем стало ясно, что этот термин применим и в других научных областях, включая информационную безопасность [Гаврюшин, с. 1–6].

При анализе воздействия человеческого фактора на информационную безопасность ключевым элементом выступает персонал организации, где деятельность сотрудников, как правило, регулируется нормами и правилами выполнения функциональных обязанностей, а отклонения от этих правил часто квалифицируются как ошибки или нарушения. Ошибка человека определяется как результат действий, не соответствующих установленным нормативным требованиям [Цыгичко и др., с. 147].

Ошибочные действия персонала, приводящие к угрозам информационной безопасности, обусловлены комплексом факторов, которые можно разделить на индивидуальные и организационные.

Индивидуальные факторы включают: психофизиологические состояния (усталость, стресс, эмоциональная нестабильность), личностные особенности (темперамент, пассивность, невнимательность), профессиональные качества (непрофессионализм, некомпетентность), этические характеристики (недобросовестность, безответственность, недисциплинированность).

Организационным факторам относятся: неблагоприятные условия труда, сверхурочная работа, недостаточная мотивация, недостаточная четкость нормативно-технической и организационно-распорядительной документации (неясность формулировок требований, обязанностей, прав и ответственности), отсутствие культуры безопасности.

Ошибочные действия сотрудников довольно трудно поддаются контролю и могут наносить большой ущерб из-за своей непредсказуемости, особенно в ситуации неопределенности.

Как отмечает Д. Канеман, ключевой проблемой становится «вариативность в суждениях» [Канеман и др., с. 169–185] – феномен, при котором решения в аналогичных ситуациях различаются из-за случайных факторов: настроения, усталости, текущей рабочей нагрузки, уровня концентрации или даже из-за погоды или времени суток. На практике это может проявляться в непоследовательности принятия решений, что ведет к уязвимостям. Например, сотрудник, находящийся в состоянии стресса или когнитивной перегрузки, с большей вероятностью проигнорирует регламент проверки вложений в электронной почте, повышая риск фишинговой атаки.

Особую категорию опасных действий составляют умышленные действия, которые направлены на нанесение ущерба или получение выгоды. Это может быть кража данных, мошенничество, саботаж или даже промышленный шпионаж. Причинами таких действий могут быть: психические отклонения, включая психические заболевания, такие как неврозы; негативные черты характера, которые проявляются в конкретной ситуации, например, завышенная самооценка, мстительность, зависть, озлобленность и т. д.; неудовлетворенность профессиональной деятельностью, например, недовольство своим положением в коллективе; шантаж со стороны третьих лиц или организаций, а также наличие других внешних факторов; корыстные интересы или идеологические установки, к примеру, идеология исламского джихада.

В заключение следует отметить, что роль персонала в обеспечении информационной безопасности организации является крайне важным условием, которое требует особого внимания и усилий со стороны руководства. Осведомленность и привлеченность персонала играют существенную роль в обеспечении безопасности информации и снижении рисков возможных угроз.

Недооценка этого аспекта может привести к серьезным последствиям, таким как утечка конфиденциальных данных, финансовые потери и ущерб репутации. Однако при правильном подходе человеческий фактор может стать не проблемой, а частью решения.

Гаврюшин Е. И. Человеческий фактор в обеспечении безопасности конфиденциальной информации // В мире права. 2002. № 2. С. 1–6. URL: http://iccta.com/prs_a_pr012002-3.shtml (дата обращения: 05.02.2025).

Канеман Д., Сибони О., Санстейн К. Р. Шум. Несовершенство человеческих суждений / пер. с англ. М.: Изд-во АСТ, 2021.

Отчет Ponemon Intsitute «Стоимость инсайдерской угрозы: глобальный отчет за 2022 год». URL: www.proofpoint.com/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf (дата обращения: 07.02.2025).

Отчет MIT Sloan «Кибербезопасность: перспективы совета директоров в 2022 году» // MIT Sloan. URL: <https://cams.mit.edu/wp-content/uploads/Board-of-Directors-Cyber-Attitudes.pdf> (дата обращения: 07.02.2025).

Отчет о глобальных рисках за 2022 год // Всемирный экономический форум. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (дата обращения: 07.02.2025).

Отчет Ростелеком-Солар «Актуальные тренды утечек информации в финансовом секторе за 2022 год» // «РТК-Солар». URL: <https://rt-solar.ru/upload/iblock/933/pi0nov4skq8bcsfmnih2mk2ajkne97g7/Aktualnye-trendy-utechek-v-bankakh-2022.pdf> (дата обращения: 05.02.2025).

Россия: утечки информации ограниченного доступа в 2022 г. : аналит. отчет // InfoWatch. URL: www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf (дата обращения: 20.02.2025).

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. URL: <https://economic.ru/lib/118237> (дата обращения: 05.02.2025).

Цыгичко В. Н., Черешкин Д. С., Смолян Г. Л. Безопасность критических инфраструктур : моногр. Изд. 2-е, стереотип. М.: ЛЕНАНД, 2021.

УДК 930.253

А. Д. Пугачева¹
Крымский федеральный университет
(г. Симферополь)

ЭТИЧЕСКИЕ АСПЕКТЫ РАБОТЫ С КОМПЛЕКСАМИ ДОКУМЕНТОВ О ЖИЗНЕДЕЯТЕЛЬНОСТИ НАСЕЛЕНИЯ РОССИИ

В статье анализируется этическая сторона работы с комплексами документов о жизнедеятельности населения России и соответствующие механизмы контроля над соблюдением этических норм при работе с ними.

¹ Научный руководитель: И. С. Башкова, канд. ист. наук, доцент КФУ.