УДК: 004.056.53

Екимов Дмитрий Александрович
Ученая степень - Студент магистратуры
Кафедра - Безопасность в инфокоммуникационных технологиях и системах связи
Название ВУЗа - Сибирский государственный университет телекоммуникаций и информатики

Научный руководитель: Попков Г. В.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В условиях активной цифровизации и широкого внедрения информационных технологий проблема обеспечения информационной безопасности приобретает особую актуальность. Несмотря на развитие технических средств защиты информации, значительная часть инцидентов информационной безопасности по-прежнему связана с действиями пользователей. В данной статье рассматривается человеческий фактор как одна из ключевых угроз информационной безопасности организаций. В статье представлена классификация преднамеренных и непреднамеренных угроз, обусловленных человеческим фактором, а также рассмотрены основные причины их возникновения. В качестве решения выявленной проблемы предложен комплекс мер, включающий организационные, технические и образовательные подходы, направленные на снижение рисков, связанных с человеческим фактором. Результаты исследования могут быть использованы при разработке и совершенствовании систем управления информационной безопасностью в организациях различного профиля.

Ключевые слова: информационная безопасность, человеческий фактор, угрозы информационной безопасности, персонал, социальная инженерия.

Современное общество характеризуется стремительным развитием информационных технологий и повсеместным использованием цифровых решений в различных сферах деятельности. Информационные системы становятся неотъемлемой частью функционирования государственных учреждений, коммерческих организаций и частных пользователей. В связи с этим возрастает значимость обеспечения информационной безопасности, направленной на защиту конфиденциальности, целостности и доступности информации.

Несмотря на активное развитие технических и программных средств защиты, статистика инцидентов информационной безопасности свидетельствует о том, что значительная их часть обусловлена действиями человека. Ошибки пользователей, несоблюдение требований информационной безопасности, а также преднамеренные нарушения со стороны персонала нередко приводят к утечкам информации, финансовым потерям и репутационному ущербу организаций. В данном контексте человеческий фактор выступает одной из наиболее сложных и трудно контролируемых угроз информационной безопасности.

В системе обеспечения информационной безопасности человек одновременно выступает как объект защиты и как потенциальный источник угроз. В отличие от технических и программных компонентов, поведение человека не поддаётся полной формализации и автоматизированному контролю, что существенно усложняет управление рисками информационной безопасности. Именно поэтому человеческий фактор рассматривается как один из наиболее уязвимых элементов информационной системы.

Под человеческим фактором в контексте информационной безопасности понимается совокупность действий, решений, поведенческих и психологических особенностей пользователей и сотрудников, которые могут оказывать влияние на уровень защищенности информации. Эти действия могут носить как непреднамеренный характер, связанный с ошибками и неосведомлённостью, так и преднамеренный, обусловленный личной заинтересованностью, конфликтами или злоупотреблением служебным положением[1].

Особенностью человеческого фактора является его двойственная природа. С одной стороны, персонал обеспечивает функционирование информационных систем, принимает решения, управляет доступом и обрабатывает данные. С другой стороны, именно человек чаще всего становится целью кибератак, основанных на методах социальной инженерии, манипулировании доверием и психологическом воздействии. Поэтому даже при наличии современных средств защиты информации недостаточное внимание к человеческому фактору может существенно снизить эффективность всей системы информационной безопасности.

Роль человеческого фактора особенно возрастает в условиях цифровой трансформации организаций, когда увеличивается количество информационных систем, расширяется удалённый доступ к корпоративным ресурсам и возрастает объём обрабатываемых данных. В таких условиях требования к уровню осведомлённости и ответственности пользователей значительно возрастают, однако на практике они часто не соответствуют реальным угрозам. Это приводит к формированию разрыва между техническим уровнем защиты и фактическим уровнем безопасности, определяемым поведением персонала.

Следует отметить, что человеческий фактор тесно связан с организационными аспектами информационной безопасности. Отсутствие чётко сформулированных политик, формальный подход к обучению

сотрудников, недостаточный контроль соблюдения регламентов создают условия, при которых даже добросовестные пользователи могут непреднамеренно нарушать требования безопасности. В результате человеческий фактор становится неотъемлемой частью общей системы рисков, требующей комплексного управления наряду с техническими и программными мерами защиты[2].

Таким образом, человеческий фактор в системе информационной безопасности следует рассматривать не как второстепенный элемент, а как ключевую составляющую, напрямую влияющую на устойчивость информационных систем к современным угрозам. Эффективное обеспечение информационной безопасности невозможно без учёта поведенческих, психологических и организационных особенностей деятельности персонала.

Практика обеспечения информационной безопасности показывает, что угрозы, связанные с человеческим фактором, отличаются большим разнообразием и проявляются на всех этапах жизненного цикла информационных систем. В отличие от технических уязвимостей, которые могут быть выявлены и устранены с помощью специализированных средств, угрозы, обусловленные действиями персонала, часто носят скрытый характер и выявляются уже после наступления инцидента.

С точки зрения практического применения целесообразно разделять угрозы информационной безопасности, связанные с человеческим фактором, на непреднамеренные и преднамеренные. Непреднамеренные угрозы возникают в результате ошибок, невнимательности или недостаточной компетентности пользователей. К таким угрозам относятся случаи использования простых или повторяющихся паролей, передача учётных данных третьим лицам, открытие вредоносных вложений в электронной почте, а также некорректная настройка программного обеспечения. Подобные инциденты широко распространены в организациях различного

профиля и, как отмечается в ряде исследований, составляют значительную долю всех нарушений информационной безопасности [1].

Одним из наиболее распространённых практических примеров непреднамеренных угроз являются фишинговые атаки, основанные на методах социальной инженерии. Злоумышленники используют доверчивость пользователей, имитируя сообщения от руководства, банков или технической поддержки. Даже при наличии антивирусных средств и систем фильтрации трафика успешность таких атак во многом определяется действиями конкретного сотрудника, принявшего решение перейти по ссылке или передать конфиденциальную информацию. Анализ инцидентов показывает, что отсутствие регулярного обучения персонала значительно повышает вероятность успешной реализации подобных атак [2].

Преднамеренные угрозы, связанные с человеческим фактором, как правило, связаны с действиями инсайдеров — сотрудников, обладающих легитимным доступом к информационным ресурсам. В практической деятельности организаций такие угрозы проявляются в виде умышленного копирования конфиденциальных данных, передачи информации конкурентам, саботажа информационных систем или злоупотребления правами доступа. Особую опасность инсайдерские угрозы представляют в крупных организациях с разветвлённой структурой доступа, где контроль действий пользователей затруднён [3].

Отдельного внимания заслуживает проблема социальной инженерии, которая занимает промежуточное положение между преднамеренными и непреднамеренными угрозами. С одной стороны, инициатором атаки является злоумышленник, действующий преднамеренно, с другой — успешность атаки напрямую зависит от ошибок или психологических особенностей сотрудников. В реальной практике нередко фиксируются случаи, когда сотрудники добровольно предоставляют злоумышленникам доступ к информационным системам, не осознавая последствий своих

действий. Данный факт подтверждает тезис о том, что человек является не только источником угроз, но и их основной целью [4].

Практический опыт показывает, что наибольший ущерб организациям наносят комбинированные угрозы, при которых человеческий фактор сочетается с техническими уязвимостями. Например, использование слабых паролей в сочетании с отсутствием многофакторной аутентификации значительно упрощает несанкционированный доступ к информационным ресурсам. В подобных случаях даже базовые организационные меры могли бы существенно снизить вероятность реализации угрозы, однако на практике им часто уделяется недостаточное внимание [5].

Таким образом, классификация угроз информационной безопасности, обусловленных человеческим фактором, позволяет не только систематизировать возможные риски, но и выявить наиболее уязвимые направления в системе защиты информации. Практика показывает, что без учёта человеческого фактора и его особенностей невозможно обеспечить устойчивую и эффективную систему информационной безопасности.

Анализ практики обеспечения информационной безопасности показывает, что угрозы, обусловленные человеческим фактором, имеют комплексную природу и, как правило, не возникают изолированно. В большинстве случаев их появление связано с совокупностью организационных, образовательных и психологических причин, усиливающих уязвимость информационных систем. Понимание данных причин является необходимым условием для разработки эффективных мер по снижению рисков информационной безопасности.

Одной из ключевых причин возникновения угроз, связанных с человеческим фактором, является недостаточный уровень осведомлённости персонала в области информационной безопасности. Во многих организациях обучение сотрудников носит формальный характер и ограничивается ознакомлением с базовыми требованиями без формирования

устойчивых навыков безопасного поведения. В результате пользователи не всегда способны распознать фишинговые сообщения, корректно оценить риски при работе с внешними носителями информации или осознать последствия нарушения установленных регламентов [2].

Существенное влияние на уровень информационной безопасности оказывает и организационная среда. Отсутствие чётко регламентированных процедур, неактуальные или избыточно сложные политики информационной безопасности, а также недостаточный контроль за их соблюдением создают условия, при которых сотрудники вынуждены искать неформальные способы выполнения рабочих задач. Подобная практика нередко приводит к использованию личных устройств, передаче служебной информации через незащищённые каналы связи и хранению данных вне корпоративных информационных систем [3].

Не менее значимой причиной является низкая мотивация персонала к соблюдению требований информационной безопасности. В условиях высокой нагрузки и жёстких сроков выполнения задач требования ИБ часто воспринимаются сотрудниками как дополнительное препятствие, а не как элемент защиты. Отсутствие системы ответственности и поощрений за соблюдение требований безопасности снижает уровень вовлечённости персонала и повышает вероятность нарушений, как непреднамеренного, так и преднамеренного характера [4].

Причины возникновения угроз, связанных с человеческим фактором, также могут быть обусловлены недостатками в системе управления доступом. Избыточные права пользователей, несвоевременное их пересмотр и отсутствие принципа минимально необходимого доступа повышают риск злоупотреблений и инсайдерских инцидентов. В случае увольнения или перевода сотрудников данные недостатки могут привести к сохранению несанкционированного доступа к критически важным информационным ресурсам [1].

Итак, анализ причин возникновения угроз, связанных с человеческим фактором, позволяет сделать вывод о том, что данные угрозы являются следствием не только индивидуальных ошибок пользователей, но и системных проблем в организации управления информационной безопасностью. Эффективное противодействие данным угрозам возможно лишь при комплексном подходе, сочетающем технические, организационные и образовательные меры, что будет рассмотрено в следующем разделе статьи.

Проведённый анализ показывает, что человеческий фактор оказывает системное влияние на уровень информационной безопасности организации и во многих случаях определяет эффективность функционирования всех применяемых средств защиты. Основная проблематика заключается в несоответствии между возросшей сложностью и масштабами информационных систем и реальным уровнем подготовки, ответственности и осознанности пользователей. Даже при наличии современных технических решений именно действия персонала нередко становятся решающим фактором успешной реализации угроз информационной безопасности.

Ключевая проблема влияния человеческого фактора на информационную безопасность состоит в том, что человек остаётся наименее формализуемым элементом системы защиты. Технические средства подчиняются заданным алгоритмам, тогда как поведение пользователей зависит от множества внешних и внутренних факторов, включая профессиональный опыт, психологическое состояние и особенности корпоративной культуры. В результате даже хорошо спроектированная система информационной безопасности может оказаться неэффективной при отсутствии должного контроля и управления человеческим фактором[2].

Практика эксплуатации информационных систем показывает, что значительная часть инцидентов информационной безопасности происходит при формальном соблюдении установленных требований. Пользователи, стремясь упростить рабочие процессы, сознательно или неосознанно обходят

механизмы защиты, используют несанкционированные программные средства и передают служебную информацию по незащищённым каналам связи. Подобные действия формируют скрытые уязвимости, которые не выявляются стандартными средствами технического контроля и обнаруживаются лишь после наступления негативных последствий.

Последствия реализации угроз, обусловленных человеческим фактором, носят комплексный характер и затрагивают различные аспекты деятельности организации. К наиболее распространённым последствиям относятся утечки конфиденциальной информации, компрометация персональных данных, нарушение целостности информационных ресурсов и снижение доступности информационных систем. Помимо прямого ущерба, связанного с восстановлением работоспособности систем, организации несут значительные финансовые и репутационные потери, а также риски привлечения к ответственности за нарушение требований законодательства в области защиты информации [2].

Особую сложность представляет проблема выявления и предотвращения угроз на ранних стадиях. В отличие от внешних атак, человеческий фактор часто не воспринимается как приоритетный источник риска, что приводит к недостаточному вниманию со стороны руководства и служб информационной безопасности. В результате меры по управлению человеческим фактором носят фрагментарный характер и не интегрируются в общую систему управления рисками.

Таким образом, проблематика влияния человеческого фактора на уровень информационной безопасности заключается не только в высокой вероятности ошибок со стороны пользователей, но и в отсутствии комплексного подхода к управлению данными рисками. Решение данной проблемы требует перехода от исключительно технической модели защиты информации к интегрированной системе, учитывающей организационные, поведенческие и образовательные аспекты деятельности персонала. В

следующем разделе статьи рассматриваются основные методы и меры, направленные на снижение рисков, связанных с человеческим фактором.

Снижение рисков информационной безопасности, обусловленных человеческим фактором, требует комплексного подхода, сочетающего организационные, технические и образовательные меры. Применение отдельных инструментов без их интеграции в общую систему управления информационной безопасностью, как правило, не обеспечивает устойчивого результата.

К числу основных организационных мер относится разработка и актуализация политик информационной безопасности, регламентирующих действия пользователей при работе с информационными ресурсами. Важную роль играет реализация принципа минимально необходимого доступа и регулярный пересмотр прав пользователей. Данные меры позволяют снизить вероятность злоупотребления полномочиями и ограничить возможный ущерб в случае инцидента.

Таким образом, эффективное снижение рисков, связанных с человеческим фактором, возможно лишь при реализации комплексной системы мер, интегрированной в общую модель управления информационной безопасностью организации. В целях снижения рисков, связанных с человеческим фактором, организациям рекомендуется внедрять системный подход к управлению информационной безопасностью, включающий регулярную оценку рисков, связанных с действиями персонала. Обучение сотрудников должно носить непрерывный характер и быть ориентировано на практические аспекты безопасной работы с информацией. Дополнительно рекомендуется использовать показатели эффективности, позволяющие оценивать уровень соблюдения требований информационной безопасности и своевременно выявлять отклонения.

В ходе проведённого исследования был рассмотрен человеческий фактор как одна из ключевых угроз информационной безопасности.

Установлено, что значительная часть инцидентов информационной безопасности обусловлена действиями персонала, как непреднамеренного, так и преднамеренного характера. Анализ причин возникновения данных угроз показал их системный характер и зависимость от организационных и поведенческих факторов. В статье предложен комплекс мер, направленных на снижение рисков, связанных с человеческим фактором. Реализация данных мер позволяет повысить уровень защищённости информационных систем и обеспечить устойчивое функционирование организаций в условиях современных информационных угроз.

Список литературы

1. Астахов А. М. Информационная безопасность: угрозы и методы защиты : учеб. пособие для вузов. — М. : Горячая линия – Телеком, 2021. — 384 с.
2. Котенко И. В., Чечулин А. А. Социальная инженерия как угроза информационной безопасности // Информационные технологии. — 2020. — № 6. — С. 45–52.
3. Бабенко Л. К. Информационная безопасность автоматизированных систем : учеб. пособие. — М. : БИНОМ. Лаборатория знаний, 2020. — 336 с.
4. Зегжда П. Д., Исаев А. В. Основы информационной безопасности : учебник для вузов. — СПб. : Питер, 2019. — 272 с.
5. Mitnick K., Simon W. The Art of Deception: Controlling the Human Element of Security. — Indianapolis : Wiley Publishing, 2017. — 368 p.
6. Bishop M. Computer Security: Art and Science. — 2nd ed. — Boston : Addison-Wesley, 2019. — 1232 p. ISO/IEC 27001:2013.
7. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. действующая).