УДК 004.056.5

Персонал как угроза информационной безопасности в компании в 2024 г.: экономические и репутационные риски

Солдатов Никита Алексеевич, студент, Сибирский государственный университет телекоммуникаций и информатики, soldatov.nikita1996@yandex.ru

В статье рассматриваются угрозы информационной безопасности, которые продолжают эволюционировать. Одной из самых серьезных проблем для компаний остаются риски, связанные с персоналом. Независимо от уровня технологической зрелости компании и принятых мер защиты, человеческий фактор продолжает оставаться основным источником угроз. В этой статье мы рассмотрим, почему персонал является такой уязвимой частью информационной безопасности, какие экономические и репутационные риски связаны с внутренними угрозами и как эффективно управлять этими рисками.

Ключевые слова: информационная безопасность, защита данных, управление персоналом, экономические риски, стратегия управления рисками.

Человеческий фактор исторически остается одной из самых серьезных угроз для информационной безопасности компании. В 2024 г. это особенно актуально, поскольку цифровизация, внедрение новых технологий и автоматизация увеличивают объемы и доступность данных, а значит, создают новые уязвимости [1].

Существует несколько типов угроз, связанных с персоналом:

1. Ошибки сотрудников. Часто сотрудники становятся источником угроз не по причине злого умысла, а из-за недостаточной осведомленности или простых ошибок. Например, неправильная настройка безопасности, открытие фишингового письма или использование слабых паролей могут привести к утечке данных или взлому системы.

2. Внутренние угрозы со стороны недобросовестных сотрудников. Не все угрозы со стороны персонала носят случайный характер. В некоторых случаях сотрудники могут намеренно разглашать информацию, передавать данные конкурентам или злоумышленникам, что приводит к утечке конфиденциальных сведений. Такие действия могут быть мотивированы личной выгодой, местью или влиянием внешних факторов.

3. Необученность и недостаток культуры безопасности. В 2024 г., несмотря на прогресс в области технологий, многие компании все еще сталкиваются с проблемами недостаточной осведомленности сотрудников о рисках информационной безопасности. Это связано с отсутствием регулярных обучающих программ, что делает персонал уязвимым для атак через социальную инженерию, фишинг и другие виды манипуляций [1].

4. Влияние удаленной работы и гибридных моделей. В последние годы, в связи с распространением удаленной работы и гибридных рабочих моделей, появляется новая угроза: утечка данных через недостаточно защищенные личные устройства сотрудников, использование нестабильных сетей и отсутствие контроля за соблюдением политики безопасности в домашних условиях. Это повышает вероятность атак и утечек информации.

Экономические риски для компании.

Угрозы, исходящие от персонала, могут не только привести к повреждению инфраструктуры, но и вызвать значительные экономические потери для компании. Рассмотрим основные экономические риски, связанные с внутренними угрозами:

1. Финансовые потери из-за утечек данных. Если сотрудник случайно или намеренно разгласит конфиденциальную информацию или данные клиентов, компания может столкнуться с высокими штрафами, как в случае с нарушением Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Штрафы могут достигать миллионов долларов, а в некоторых случаях они сопровождаются дополнительными издержками на расследования и компенсацию ущерба.

2. Прямые убытки от утраты данных или взлома системы. Вредоносные действия сотрудников или их ошибки могут повлечь за собой утрату важных данных, что приведет к значительным финансовым потерям. Это может включать потерю клиентской базы, разрушение репутации или уничтожение интеллектуальной собственности компании.

3. Затраты на восстановление после инцидента. После инцидента с утечкой или взломом компании требуется время и ресурсы для восстановления. Это включает в себя восстановление данных, модернизацию систем безопасности, расследование инцидента и компенсацию ущерба пострадавшим сторонам. Все эти процессы требуют значительных финансовых вложений.

4. Увольнение и компенсации. При выявлении недобросовестного поведения со стороны сотрудника (например, кражи данных) компания понесет не только репутационные потери, но и затраты на юридическое разбирательство, увольнение сотрудника, возможные компенсации и поиск замены [2].

Репутационные риски для компании.

Репутационные риски, связанные с угрозами со стороны персонала, могут быть даже более разрушительными, чем экономические потери. В условиях высококонкурентного рынка информация о нарушении безопасности может мгновенно стать публичной и нанести ущерб репутации компании. Рассмотрим несколько репутационных рисков:

1. Утечка персональных данных клиентов или корпоративной информации может серьезно подорвать доверие к компании. Для организаций, работающих с конфиденциальной информацией, такой инцидент часто приводит к потере клиентов и партнеров, а также снижает способность привлекать новых деловых партнеров. Это особенно критично для компаний, где доверие и защита данных играют ключевую роль в поддержании деловых отношений.

2. Ухудшение имиджа на рынке. Это может снизить интерес инвесторов, партнеров и потребителей, что в долгосрочной перспективе потенциально приведет к снижению доходов и рыночной стоимости компании.

Неправомерные действия сотрудников, такие как кража интеллектуальной собственности или утечка секретной информации, могут нанести ущерб имиджу бренда компании [3].

Стратегии управления рисками, связанными с персоналом.

Для минимизации экономических и репутационных рисков, связанных с персоналом, компании должны внедрять комплексные

меры безопасности и развивать культуру информационной безопасности:

1. Обучение сотрудников. Регулярные тренинги по вопросам информационной безопасности для всех сотрудников — от руководства до новичков — являются важной мерой защиты от угроз, связанных с человеческим фактором. Сотрудники должны понимать угрозы фишинга, социального инжиниринга и правила работы с конфиденциальной информацией.

2. Мониторинг и аудит. Регулярный мониторинг активности сотрудников, а также проведение аудитов информационной безопасности помогает вовремя выявить и предотвратить угрозы. Важно внедрить систему контроля доступа и логирования для отслеживания действий пользователей в критичных системах.

3. Модели поведения и политика безопасности. Разработка и внедрение четкой политики безопасности, которая регулирует не только технические, но и организационные аспекты защиты данных, поможет создать безопасную рабочую среду. Важно, чтобы сотрудники знали свои обязанности и ответственность за нарушение политики.

4. Технологические меры защиты, такие как шифрование данных, двухфакторная аутентификация и системы предотвращения утечек данных (DLP), являются важными инструментами для снижения рисков, связанных с несанкционированным доступом и утечками информации. Эти меры позволяют повысить уровень безопасности, защищая данные от атак и минимизируя угрозы утечек, что особенно важно для организаций, работающих с конфиденциальной информацией.

Таким образом, персонал продолжает оставаться одним из главных источников угроз для информационной безопасности компании в 2024 г. Человеческий фактор может привести как к случайным ошибкам, так и к преднамеренным действиям, что создает серьезные экономические и репутационные риски. Для эффективного управления этими рисками компании необходимо внедрить комплексный подход, включающий обучение сотрудников, системы мониторинга и контроля, а также развитие культуры безопасности на всех уровнях.

Примечания

1. Международный стандарт ISO/IEC 27001:2022. URL: https://pqm-online.com (дата обращения: 30.12.2024).
2. Защита информации и организация аналитической работы на предприятии. URL: http://all-ib.ru (дата обращения: 30.12.2024).
3. Баранова Е. К., Бабаш А. В. Основы информационной безопасности: учебник. М., 2019. 202 с.

English version

Personnel as a threat to information security in a company in 2024: economic and reputational risks

Soldatov Nikita Alekseevich, student, Siberian State University of Telecommunications and Information Science

The article examines information security threats that continue to evolve. One of the most serious problems for companies remains the risks associated with personnel. Regardless of the level of technological maturity of the company and the measures taken to protect it, the human factor continues to be the main source of threats. In this article, we will consider why personnel are such a vulnerable part of information security, what economic and reputational risks are associated with internal threats and how to effectively manage these risks.

Keywords: information security, data protection, personnel management, economic risks, risk management strategy.