Секция «10.5 Компьютерное право и информационная безопасность»

Правовые меры противодействия угрозам социальной инженерии в корпоративной среде

Научный руководитель – Морозов Андрей Витальевич

Романов Владимир Павлович
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Москва, Россия
E-mail: v.romanov1310@gmail.com

В условиях стремительной цифровизации и усложнения архитектуры корпоративных систем основным вектором атак становится «человеческий фактор». Социальная инженерия, представляющая собой совокупность методов психологического воздействия на сотрудников для получения несанкционированного доступа к конфиденциальной информации, сегодня признается одной из наиболее деструктивных угроз. Особенность данной угрозы заключается в том, что она направлена на эксплуатацию когнитивных искажений персонала, что делает традиционные технические средства защиты (SIEM-системы, антивирусное ПО) недостаточно эффективными без соответствующего правового сопровождения.

Эффективное противодействие угрозам социальной инженерии требует выстраивания комплексной системы организационно-правовых мер. Первоочередной задачей является легитимизация требований информационной безопасности во внутренних документах организации. Необходимо детальное закрепление правил «цифровой гигиены» в Правилах внутреннего трудового распорядка (ПВТР) и Положении о защите коммерческой тайны. Важно, чтобы обязанности по соблюдению регламентов ИБ были интегрированы непосредственно в должностные инструкции сотрудников. С юридической точки зрения это создает правовое основание для привлечения работника к дисциплинарной или материальной ответственности в случае совершения им действий, повлекших за собой инцидент безопасности (например, переход по фишинговой ссылке или разглашение аутентификационных данных третьим лицам).

Особое внимание в рамках исследования уделяется правовому регулированию процедур превентивного контроля, таких как «имитированные фишинговые атаки». Подобные мероприятия должны проводиться на строгой правовой основе, чтобы исключить риски нарушения конституционных прав граждан на неприкосновенность частной жизни и тайну переписки. Автор предлагает внедрение регламента предварительного уведомления сотрудников о возможности проведения подобных проверок в рамках трудового договора, что позволяет соблюсти баланс интересов работодателя и работника.

Кроме того, в системе государственного аудита и корпоративного контроля возрастает роль комплаенс-процедур. Существует необходимость перехода от формального ознакомления сотрудников с инструкциями к созданию юридически значимых механизмов непрерывного обучения (Security Awareness). Правовое закрепление периодичности таких тренингов и фиксация результатов тестирования позволяют организации сформировать доказательственную базу на случай судебных разбирательств, связанных с утечками данных по вине персонала.

Таким образом, правовое обеспечение информационной безопасности в части борьбы с социальной инженерией должно трансформироваться в динамическую систему управления рисками. Сочетание четких локальных нормативных актов и механизмов контроля позволяет не только минимизировать вероятность успешных атак, но и обеспечить правовую защищенность бизнеса в условиях современных киберугроз.

Источники и литература

1) Бачило И.Л. Информационное право: учебник для вузов. М.: Юрайт. 2024.
2) Волков А.А. Психологические методы социальной инженерии и правовые способы защиты от них // Вестник компьютерного права. 2025, №3.
3) Полякова Т.А. Правовое обеспечение информационной безопасности при использовании облачных технологий // Труды по интеллектуальной собственности. 2024, Т. 48, № 1.
4) Росс Г.В. Информационные системы в государственном аудите. М.: Экономика. 2023.
5) Mitnick K.D. The Art of Deception: Controlling the Human Element of Security. Wiley Publishing. 2002.