Глава 1. Предпосылки для управления информационными рисками

написано Александр Астахов | 10 июня, 2023

> *«Обязанность ученых – очищать мировоззрение современников от заблуждений».*
>
> *Н.К. Кольцов, известный генетик*

- Риски, породившие мировой финансовый кризис
- Информационные риски киберпространства
- Обилие стандартов, требований, средств и технологий защиты не уменьшает риски
- Государственное регулирование только создает дополнительные риски
- Оценка рисков как основа корпоративного управления
- Как оценивают риски наши соотечественники

Возможно, для кого-то это и будет новостью, однако анализ ситуации в стране и в мире показывает, что без управления рисками уже невозможно обеспечить стабильность и избежать глобальных кризисов. В этой вступительной главе мы попытаемся осознать важность управления рисками, а также те проблемы, которые решаются путем оценки риска.

Из дальнейшего изложения следует, что уже в наши дни многим организациям управлять рисками совершенно необходимо не только для получения конкурентных преимуществ, но и для выживания. Однако у читателя может возникнуть резонный вопрос: «Раз это столь важно, тогда каким же образом многие организации до сих

пор обходились и обходятся без систематического управления рисками?» На наш взгляд, все дело в том, что времена очень быстро меняются. Раньше управление рисками действительно было не столь актуально из-за незначительного количества информационных угроз, а также ограниченности существовавших тогда технологий и стандартов. Выбирать контрмеры было особенно не из чего, да и защищаться тоже было не от чего.

Сейчас же мир стремительно меняется. Для нового информационного века характерны немыслимые ранее угрозы и кризисы. Количество вредоносных кодов сейчас исчисляется миллионами, а количество известных интернет-уязвимостей, уязвимостей системного и прикладного ПО – десятками тысяч. Ежедневно регистрируется огромное количество сетевых атак и внутренних инцидентов информационной безопасности. Сложность атак, изощренность способов их реализации и степень опасности возрастает в геометрической прогрессии.

Все это могло бы быть не более чем забавно, если бы столь же стремительно не увеличивалась зависимость критичной для жизнедеятельности людей инфраструктуры и бизнеса от информационных технологий. Взлом очередного веб-сайта может послужить развлекательной новостью и темой для обсуждения в узком кругу посвященных, DDoS-атака (распределенная атака на отказ в обслуживании) против сайтов крупного информационного агентства – это уже новость, получающая более широкий резонанс. Скоординированные атаки на объекты инфраструктуры: электростанции, телекоммуникационные узлы, системы водо-, тепло- и газоснабжения – могут стать причиной глобальной катастрофы, последствия которой даже трудно себе представить.