Типичные ошибки при управлении рисками

написано Александр Астахов | 11 июня, 2023

Типичные ошибки в управлении рисками ИБ, которые автору приходилось наблюдать, обычно, сводятся к следующему:

1. Для оценки рисков за большие деньги приобретается какой-либо программный инструментарий, а потом выясняется, что он не подходит, не соответствует требованиям стандартов, не интегрируется в систему управления бизнес-рисками организации (ERM), не удобен в использовании, не позволяет количественно оценить риски, не позволяет стоить приемлемые модели активов, угроз, нарушителей и уязвимостей, не учитывает силу имеющихся механизмов контроля, не позволяет создавать нужных отчетов, не предоставляет возможностей представителям бизнеса классифицировать информационные активы и оценивать их ценность, вместо информационных активов почему-то оперирует любыми другими активами (помещения, оборудование, кадры, процессы, рабочие задачи), ни с чем не совместим и использует закрытые интерфейсы и т.п.
2. Проводится слишком высокоуровневая оценка рисков, не предоставляющая достаточного объема достоверной информации для принятия управленческих решений по вопросам ИБ. Вместо отдельных бизнес-процессов рассматриваются лишь общие направления деятельности (продажи, производство, бухгалтерский учет и т.п.), вместо информационных активов, рассматриваются лишь классы активов (например, проектная документация, бухгалтерская документация, клиентская информация и т.п.), вместо конкретных угроз безопасности рассматриваются классы угроз (например, НСД к информации, атаки на отказ в обслуживании, выход их строя технических средств и т.п.). На выходе получается

примерно следующее: «в случае НСД к клиентской информации компания может понести значительный ущерб в результате потери части клиентов». А кто-то в этом сомневался? На выходе такой оценки рисков получается информация, которая итак всем была известна еще до начала данного процесса. Делается вывод о том, что оценка рисков лишена смысла, т.к. не дает никакой полезной информации.

3. Проводится слишком детализированная оценка рисков, которая бросается на полпути, из-за невозможности ее практической реализации. Например, делается попытка оценить риски для каждой порции информации (файла, записи в БД, бумажного документа) или рассматривается сотня различных сценариев реализации НСД к файловому серверу с использованием различных уязвимостей TCP/IP стека. Бессмысленность подобных стараний довольно скоро становится очевидной для всех участников процесса и делается вывод о том, что оценка рисков вообще слишком сложна и не имеет практического смысла.
4. Оцениваются риски не информационных активов, а любых других активов, прямо или косвенно связанных с информационными либо являющиеся комбинацией информационных активов и прочих активов (например, люди, помещения, оборудование, приложения, задачи, процессы, рабочие места, системы и т.п.). В результате весь анализ уходит немного в сторону от ИБ в вопросы делопроизводства, управления кадрами, физическую и экономическую безопасность, организацию бизнес-процессов и куда угодно еще. Вместо информационной безопасности получается системная безопасность, процессная безопасность, физическая безопасность, кадровая безопасность и т.д. Риски ИБ перемешиваются с остальными бизнес-рисками и вопрос становится слишком сложными, а выводы делаются те же, что и в предыдущих случаях – о практической нецелесообразности применения риск-ориентированного подхода.
5. Бизнес-подразделения не вовлекаются в процесс оценки

рисков, либо к ним обращаются с бессмысленными вопросами о том, сколько стоит их информация (вместо того, чтобы обсуждать с ними конкретные понятные им бизнес-ситуации, возникающие как следствие инцидентов ИБ). Поскольку дать разумный ответ на подобные вопросы невозможно, на этом участие представителей бизнеса в оценке рисков заканчивается и остается только раздражение. Далее делается вывод о том, что стоимость информационного актива объективно оценить нельзя, а значит нельзя оценить соответствующие риски.

6. Оценкой рисков занимается исключительно служба ИБ без привлечения представителей бизнес-подразделений (которые не могут сказать сколько стоит их информация). Все риски ИБ при этом завышаются, что вызывает иронию, либо негодование у руководства компании, которое чувствует, что его пытаются развести на деньги.
7. Используется слишком упрощенный подход к оценке рисков, например, учитывается только вероятность угрозы и размер ущерба (причем только качественные оценки), при этом уязвимости и механизмы контроля отдельно не рассматриваются и не учитываются их взаимосвязи и относительная сила.
8. Процессы оценки и обработки рисков ИБ оторваны от реальных процессов принятия управленческих решений руководством организации, не влияют на внутренние политики, не учитываются при бюджетировании и т.п.