Отчет об оценке рисков

написано Александр Астахов | 10 июня, 2023

Отчет об оценкерисков необходим для руководства и всех заинтересованных сторон, вовлеченных в процесс управления рисками. Другими словами, этот документ нужен для коммуникации рисков. Результаты оценки рисков могут служить предметом рассмотрения на заседании Управляющего комитета по информационной безопасности.

_____

Краткая структура отчета об оценке рисков:

- *Введение*

– *Основания, общие сведения*

– *Цели и задачи*

- *Методология и результаты*

– *Идентификация активов и требований*

– *Оценка активов и последствий*

– *Анализ угроз и уязвимостей*

– *Вычисление и оценивание рисков*

- *Резюме рисков для руководства*

– *Описание самых высоких рисков и причин их существования*

- *Приложения*

– *Реестры активов, требований и рисков*

– *Таблицы определения ценности активов и ущерба для бизнеса*

Отчет об оценке рисков обычно включает в себя введение, краткое описание используемой методологии оценки рисков со ссылкой на соответствующие приложения и резюме рисков.

Важнейшей частью этого отчета является резюме рисков, адресованное руководству организации принимающему решения по рискам. В этом разделе в краткой повествовательной форме описываются самые высокие риски организации, на которые руководству следует обратить первоочередное внимание, с указанием ожидаемого среднегодового ущерба и перечислением уязвимостей, способствующих реализации данных рисков. По всем остальным рискам, оценочный уровень которых ниже, читатели отчета переадресуются к реестру информационных рисков.

Отчет об оценке рисков, как и другие документы по рискам, должен носить конфиденциальный характер и защищаться от несанкционированного доступа, наряду с другими секретами.

Конечно, на этом оценка рисков не заканчивается. Высокоуровневая оценка позволила расставить необходимые приоритеты, выявив и обосновав те группы рисков и механизмов контроля, которые имеют наибольшее значение. Для организаций с относительно невысокой степенью зависимости от информационных технологий этого уже может оказаться достаточно. Для остальных организаций потребуется дальнейшая детализация угроз, уязвимостей и механизмов контроля, в результате чего количество рассматриваемых групп рисков может возрасти с нескольких десятков до нескольких сотен.