Реализация пилотного проекта по оценке рисков

написано Александр Астахов | 11 июня, 2023

*После завершения документирования СУИР*необходимо определить *первоначальную область оценки рисков*, которая будет являться подмножеством *области действия СУИБ* вашей организации. Не следует сразу браться за оценку всех возможных рисков для всех информационных активов, находящихся в области действия СУИБ. Вместо этого рекомендуется выбрать несколько наиболее критичных активов для реализации пилотного проекта по оценке рисков.

В ходе реализации пилотного проекта отдельные аспекты *методологии оценки рисков* должны быть доработаны и приспособлены к особенностям организации.

Вторая редакция методологии оценки рисков, разработанная по результатам выполнения пилотного проекта, должна быть согласована и утверждена на совещании экспертной группы. На этом этапе может быть принято решение о необходимости использования специализированного программного инструментария для оценки и управления рисками. При выборе такого инструментария следует руководствоваться рекомендациями стандарта BS 7799-3, а также следующими соображениями:

- Инструментарий для оценки рисков должен реализовывать полноценную методологию оценки рисков в соответствии с требованиями ISO 27001 и BS 7799-3, включая подготовку реестра информационных рисков, декларации о применимости механизмов контроля, проведение анализа расхождений, разработку плана обработки рисков.
- Используемая модель активов не должна ограничиваться только информационными активами, а также должна учитывать кадровые ресурсы, процессы, технические и программные средства.

- Должны учитываться как технические, так и организационные уязвимости, как логические, так и физические угрозы.
- Должна иметься возможность определения собственных видов активов, угроз и уязвимостей, а также форматов отчетных документов, т.е. инструмент должен быть кастомизируемым.
- Должна иметься возможность сравнения между собой результатов оценки рисков.

В случае использования специализированного программного инструментария для оценки рисков, необходимо внести соответствующие изменения в методологию оценки рисков, чтобы привести ее в соответствие с выбранным инструментарием.