Взаимосвязь процессов аудита и управления рисками

написано Александр Астахов | 10 июня, 2023

Должен быть разработан график проведения независимой стороной регулярных внутренних аудитов. Независимая сторона не обязательно должна быть внешней по отношению к организации. Аудиты, проводимые внешним органом, являются обязательными для прохождения сертификации по ISO 27001, а также для акционерных обществ, финансовых организаций и других организаций согласно требованиям законодательства. Внутренние аудиторы не должны быть подконтрольны тем, кто несет ответственность за повседневное управление СУИБ. В случае, когда при внутренних аудитах обнаруживается необходимость в принятии мер по корректировке СУИБ, эти меры должны быть документированы в полном объеме, а также должна быть определена ответственность и установлены сроки.

Набор мероприятий, проводимых при оценке рисков и при комплексном аудите, в значительной степени совпадает.

Задачи аудита:

- *идентификация активов, угроз и уязвимостей;*
- *оценка уровня защищенности;*
- *оценка соответствия требованиям;*
- *выработка рекомендаций по повышению уровня защищенности и ликвидации уязвимостей.*

Для проведения аудита необходимы требования и критерии, выработанные в ходе оценки рисков. Для оценки рисков необходимо проведение мероприятий по аудиту. Это два

параллельных процесса, обменивающихся информацией между собой. Один не может существовать без другого. Поэтому во многих случаях аудит включает в себя оценку и обработку рисков, а оценка рисков предполагает проведение аудита.

Задачи управления рисками:

- *оценка активов, угроз и уязвимостей;*
- *оценка уровней рисков;*
- *оценка рисков несоответствия требованиям;*
- *принятие решений по обработке рисков.*

Если же аудит не включает в себя оценку рисков, тогда речь идет либо об оценке соответствия конкретным нормативным документам, либо об узкой области аудита, когда, например, требуется оценить защищенность конкретной системы или приложения в отношении внешних угроз.

При рассмотрении безопасности организации в комплексе, аудит и оценка рисков — это фактически составные части одного процесса.