Документация системы управления информационными рисками

написано Александр Астахов | 11 июня, 2023

Документирование СУИР– непростая задача. Каждой организации придется разработать собственный комплект документации, отражающей структуру организации, а также ее подходы к оценке и управлению рисками. Для этих целей можно воспользоваться существующими методологиями и готовыми комплектами документов (см. Приложение № 11). Это поможет сэкономить массу времени, однако останется еще много работы.

Опасность, связанная с использованием готовых шаблонов, заключается в том, что это может лишить организацию истинного понимания того, что она делает. Так часто происходит, когда берутся на вооружение чужие наработки без учета собственного опыта.

Любые комплекты документов, впрочем как и любые продукты в области управления рисками, не являются исчерпывающими и в одинаковой степени применимыми ко всем организациям. Их состав и содержание могут меняться в зависимости от конкретных особенностей и потребностей организации.

При заполнении форм и таблиц оценки факторов риска организация должна стараться формулировать собственные правила, исходные данные и результаты как можно точнее, с привязкой к конкретным активам, сервисам, площадкам, людям, уязвимостям и т.п. Следует избегать общих фраз и выражений, заменяя их более конкретными формулировками и письменными пояснениями, чтобы все заинтересованные лица имели возможность разобраться в результатах проведенной оценки рисков и, при желании, проверить полученные выводы.

Процесс внедрения СУИР следует начинать с внимательного

изучения проектов документов и их обсуждения на совещании членов экспертной группы.

По результатам первоначального обсуждения должен быть сформирован подробный перечень замечаний и необходимых доработок. Доработка документов должна производиться экспертом по оценке рисков, риск-менеджером, менеджером по информационной безопасности либо совместными усилиями членов экспертной группы.

На следующем совещании экспертной группы должна быть согласована и утверждена первая редакция *Политики управления рисками* и *Методологии оценки рисков* со всеми приложениями.

Разработанная экспертной группой Политика управления рисками должна быть утверждена Управляющим комитетом по информационной безопасности в качестве одного из основополагающих внутренних нормативных документов организации и введена в действие приказом руководителя организации.