Требования к эксперту по оценке рисков

написано Александр Астахов | 10 июня, 2023

В то время как риск-менеджер контролирует функционирование СУИР в целом, стержневые процессы, такие как оценка и обработка рисков, могут выполняться отдельным экспертом или рабочей группой.

Эксперт по оценке рисков (члены рабочей группы) должен отвечать следующим требованиям:

- базовое понимание того, как функционирует бизнес, и склонности этого бизнеса к риску;
- понимание основных концепций риска, например, каким образом комбинируются оценки угрозы, уязвимости и ущерба для получения величины риска;
- понимание ИТ на уровне, достаточном для понимания угроз и уязвимостей ИТ, например, что представляют собой системы, рабочие станции, устройства хранения, операционные системы, приложения, сети передачи данных, веб-сайты, вирусы и черви, а также, каким образом они функционируют и взаимодействуют;
- понимание различных типов механизмов безопасности, как они работают и любые свойственные им ограничения, например, межсетевые экраны, системы обнаружения вторжений, механизмы идентификации и аутентификации, механизмы контроля доступа, шифрование, средства видеонаблюдения, а также журналирование и мониторинг и т.п.;
- практическое понимание используемой методологии оценки рисков и любых, связанных с ней инструментов, программного обеспечения или форм;
- аналитические способности, т.е. способность выделять относящиеся к делу факты;

- способность идентифицировать в организации людей, которые смогут предоставить необходимую информацию;
- уровень коммуникабельности, достаточный для получения необходимой информации от людей в организации и сообщения о результатах оценки рисков в форме, понятной руководству, принимающему решения.

Эксперт по оценке рисков должен быть профессионалом в области ИТ либо информационной безопасности. Он также может быть «человеком из бизнеса» при условии, что он обладает необходимыми знаниями и квалификациями, перечисленными выше, либо он может являться внешним консультантом.