Жизненный цикл управления рисками

написано Александр Астахов | 11 июня, 2023

Выбранная методология оценки рисков должна обеспечивать формирование экономически обоснованной системы механизмов контроля информационной безопасности, описанных в стандарте ISO 27002 и других источниках.

Следует реализовать полный цикл управления рисками в соответствии с требованиями стандарта BS 7799-3, определяющего процессную модель СУИР, а также обеспечить управление документами и записями в рамках СУИР в соответствии с принятыми в организации процедурами.

BS 7799-3 определяет процессы оценки и управления рисками как составной элемент системы управления организации, используя ту же процессную модель, что и другие стандарты управления, которая включает в себя четыре группы процессов: *планирование*, *реализация*, *проверка*, *действие (ПРПД)*. В то время как ISO 27001 описывает общий непрерывный цикл управления безопасностью, в BS 7799-3 содержится его проекция на процессы управления информационными рисками.

В СУИР *на этапе планирования* определяются политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

*На этапе реализации*производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Руководством организации принимается *одно из четырех* решений по каждому идентифицированному риску: *принять*, *избежать*, *передать внешней стороне* либо *уменьшить*. После этого разрабатывается и

внедряется *план обработки рисков*.

*На этапе проверки*отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.