Анализ угроз и уязвимостей

написано Александр Астахов | 10 июня, 2023

Активы являются объектом для многих видов угроз. Угроза может стать причиной нежелательного инцидента, в результате которого организации будет причинен ущерб. Этот ущерб может возникнуть в результате атаки на информацию, принадлежащую организации и приводящей к ее несанкционированному раскрытию, модификации, повреждению, уничтожению, недоступности или потери. Угрозы могут исходить от случайных или преднамеренных источников или событий. При реализации угрозы используется одна или более уязвимостей систем, приложений или сервисов. Угрозы могут исходить как изнутри организации, так и извне. Примеры угроз приведены в Приложении № 5.

Угрозы информационной безопасности на редкость разнообразны. Сориентироваться в этом разнообразии помогают перечни угроз, приведенные в приложениях к стандартам BS 7799-3 и ISO 27005. Одно из наиболее детальных описаний тысяч угроз информационной безопасности можно встретить в открытом немецком стандарте BSI IT Baseline Protection Manual (Базовое руководство по защите ИТ).

Для каждого информационного актива или группы активов определяется список угроз в отношении конфиденциальности, целостности и доступности. За основу берется модель угроз, являющаяся частью Концепции обеспечения информационной безопасности организации.

Для каждой идентифицированной угрозы определяется список уязвимостей, благодаря которым становится возможным реализация угрозы. При этом учитываются результаты аудитов безопасности и контроля защищенности информационных систем организации, влияние человеческого фактора, а также факты отсутствия или слабости применяемых механизмов контроля (организационных и технических). Примерный перечень типовых уязвимостей приведен в Приложении № 6.

На некоторой стадии, либо перед началом мероприятий по оценке рисков, либо перед началом идентификации угроз и уязвимостей, должны быть идентифицированы уже реализованные механизмы безопасности. Это необходимо для полной идентификации и реалистичной оценки угроз и уязвимостей, а также важно при рассмотрении вариантов обработки рисков и мероприятий по управлению рисками.