Нужен ли для управления рисками специальный программный инструментарий?

написано Александр Астахов | 11 июня, 2023

Замкнутый круг, связанный с выбором программного инструментария для оценки рисков, заключается в том, что имеющиеся на рынке программные продукты профессионалу не очень-то и нужны, а для начинающего специалиста они, скорее, усложнят и без того непростую задачу.

Мы считаем, что разработку и внедрение системы управления рисками неправильно начинать с выбора программного инструментария, т.к. на этой стадии вы еще не в состоянии адекватно сформулировать требования и определить потребность вашей организации в таком инструментарии. В последующем намного проще будет адаптировать вашу методику для использования специализированного инструментария, нежели адаптировать инструментарий под вашу методику. Последнюю задачу решить практически невозможно. Ни международные стандарты, ни существующий передовой опыт в области управления рисками не требуют применения программного инструментария. Поэтому лучше будет отложить это задачу на потом.

Рекомендуется сначала внедрить в организации политику управления рисками и методологию оценки рисков и провести первоначальную высокоуровневую оценку рисков вручную, в соответствии с принятой методологией. Только после этого имеет смысл переходить к выбору инструментария, который бы соответствовал используемому вами подходу и облегчал бы выполнение основных операций по оценке рисков. Вполне возможно, что специализированный программный инструментарий для оценки рисков вам и не понадобится.

Излагаемая здесь методология оценки рисков не требует

применения какого-либо специализированного программного инструментария, хотя при ее разработке и учитывался опыт работы со многими популярными программными продуктами, речь о которых пойдет ниже. Начав с использования специализированных продуктов, мы постепенно пришли к своей «табличной» методике, для применения которой не требуется никаких программных средств, кроме текстового редактора, которая полностью отвечает нашим потребностям и одновременно является достаточно простой и эффективной.

Однако и в нашей методологии существует ряд рутинных аналитических задач, связанных с формированием реестра и плана обработки рисков, а также отчетов и промежуточных рабочих документов, которые допускают возможность автоматизации. При проведении высокоуровневой оценки рисков, при которой рассматриваются порядка несколько десятков основных групп рисков, такая автоматизация позволила бы нам экономить по нескольку человеко-дней на каждом проекте, что весьма неплохо и составляет порядка 10% наших трудозатрат. Остальные 90% трудозатрат при оценке и обработке рисков приходятся не на работу с таблицами, а на сбор информации, анализ защищенности информационных систем, проведение интервью и совещаний, обсуждение и согласование конечных и промежуточных результатов. Тем не менее экономия до 10% себестоимости работ в каждом проекте – это весьма неплохой результат, конечно, при условии, что применяемый программный инструментарий полностью соответствует нашим требованиям, а не затрудняет работу, как это случается на практике.

Положительный эффект от использования программного инструментария может быть значительно выше при детализированной оценке, предполагающей рассмотрение нескольких сотен или даже тысяч рисков, т.к. в этом случае аналитическая работа существенно усложняется. В процессе оценки рисков мы проходим ряд последовательных этапов, периодически откатываясь назад, например, переоценивая определенный риск после выбора способа его минимизации. На

каждом этапе необходимо иметь под рукой опросники, перечни угроз и уязвимостей, реестры ресурсов и рисков, документацию, протоколы совещаний, стандарты и руководства. В связи с этим нужен некий запрограммированный алгоритм рабочего процесса, база данных и интерфейс для работы с этими разнообразными данными. Благодаря использованию инструментария есть возможность упорядочить хранение данных и работу с моделью активов, профилями угроз, перечнями уязвимостей и рисками, унифицировать методологию и упростить использование результатов для переоценки рисков и обеспечить воспроизводимость результатов.

Плюсы использования программного инструментария для оценки рисков:

- *автоматизация алгоритма процесса оценки и управления рисками;*
- *унификация методологии оценки рисков, обеспечивающая воспроизводимость результатов;*
- *интеграция с ERM-системами;*
- *построение и поддержание реестров активов, требований, угроз и рисков;*
- *автоматическое формирование Планов обработки рисков и Деклараций о применимости;*
- *интеграция со средствами контроля соответствия и со средствами анализа уязвимостей.*

Программные средства оценки рисков потенциально могли бы развиваться в сторону их интеграции с другими программными системами и средствами защиты информации, например со средствами инвентаризации информационных активов, сетевыми и хостовыми сканерами, средствами контроля соответствия требованиям, системами планирования и бюджетирования и т.п.

Помимо средств оценки и управления рисками программный инструментарий может предоставлять дополнительные возможности для документирования СУИБ, анализа расхождений с требованиями стандартов, формирования и сопровождения реестра активов и другие полезные функции, необходимые для внедрения и эксплуатации СУИБ. В результате некоторые средства оценки рисков эволюционизируют в системы управления жизненным циклом СУИБ, автоматизирующие документооборот, и контрольные функции. Примерами таких программных продуктов являются рассматриваемые далее Callio Secura 17799 и Proteus Enterprise. Эти продукты были выбраны только в качестве примера. Не следует относится к их рассмотрению здесь, как к нашей рекомендации приобретать именно этот продукт либо продукты с аналогичной функциональностью. Приводимые далее сравнения и описания продуктов основаны исключительно на нашем личном опыте и предназначены лишь для того, чтобы дать читателю начальное представление о современных средствах управления информационными рисками.