Профили рисков информационной безопасности

написано Александр Астахов | 11 июня, 2023

Профиль рисков ИБ (ПР) – документ, характеризующий риски ИБ объекта защиты (ОЗ). В качестве объекта защиты выступает информационная система. Здесь можно провести аналогию с Профилями защиты (ПЗ), определяемым стандартом ISO 15408, определяющими требования к объектам оценки (ОО) с учетом предположений об условиях функционирования ОО и задач по безопасности. Профиль рисков – определяет риски ИБ для ИС, способы их обработки и требования по ИБ, обусловленные существующими рисками и способами их обработки. Будут разрабатываться как частные ПР, описывающие информационные риски и состояние их обработки, в конкретных организациях и ИС, так и типовые ПР, которые будут общедоступны и будут публиковаться на этом сайте.

В практике таможенных органов, например, используется следующее определение профиля риска (не ИБ): «Профиль риска это – совокупность сведений об области риска, индикаторов риска, а также указания о применении необходимых мер по предотвращению или минимизации риска».

Профиль информационных рисков имеет следующую структуру:

Введение
Контекст управления рисками
– Цели управления рисками
– Критерии оценки ущерба
– Критерии оценки рисков
– Критерии принятия остаточных рисков
– Область и границы оценки рисков
– Организационная структура управления рисками
Активы
– Бизнес-процессы

– Информационные активы
– Ценность активов
Угрозы
– Модель нарушителя
– Модель угроз
– Профили и жизненные циклы угроз
– Оценка вероятности угроз
Уязвимости
– Организационные уязвимости
– Технические уязвимости
– Оценка уровня уязвимостей
Контрмеры
– Организационные контрмеры
– Технические контрмеры
– Оценка эффективности контрмер
Риски
– Матрица оценки риска
– Шкала оценки риска
– Реестр информационных рисков
– План обработки рисков
Оценка возврата инвестиций
– Стоимость контрмер
– Экономический эффект
– Коэффициент возврата инвестиций
Указания по применению

Структура ПР отражает весь процесс оценки и обработки рисков, поэтому частные профили рисков у нас уже есть. Их можно сделать из отчетов по результатам соответствующих проектов. Типовые ПР будут носить отраслевой характер. Для их разработки и согласования надо будет привлекать регуляторов и отраслевых экспертов.

Понятие Профиля риска мне пока в области ИБ не встречалось, мы его впервые вводим в нашей глобалтрастовской методологии управления рисками, базирующейся на ISO 2700x (описанию этой методологии посвящена моя книга, опубликованная на сайте

http://анализ-риска.рф). Надеюсь, что разработка ПР будет поддержана и их потенциальными пользователями и регуляторами и интеграторами. Не дожидаясь этого счастливого момента, мы будем разрабатывать типовые ПР на нашем практикуме по анализу рисков http://globaltrust.ru/obuchenie/avtorskie-uchebnye-kursy/is002s-master-klass-praktikum-po-ocenke-riskov-informacionnoi-bezopasnosti

Экспертному сообществу уже порядком надоела безумная гонка нормативных документов и требований ИБ. На ничем не прикрытые головы сотрудников подразделений ИБ организаций вываливается все усиливающийся поток руководящих указаний, положений, стандартов, рекомендаций, методик и т.п., содержащих не связанные между собою, зачастую произвольным образом собранные требования, на 90% дублирующие друг друга (переписываемые из одного стандарта в другой), в каких-то местах противоречащие самим себе, в каких-то другим требованиям, в каких-то существующей практике и здравому смыслу. Об обосновании этих требований и речи не идет. Почему именно эти требования, почему именно в такой последовательности и именно в такой формулировке, какие угрозы и в какой степени они должны предотвращать? Излишнее усердие в нормотворчестве не решает реальных проблем ИБ и лишь создает новые. Службы ИБ должны в основном заниматься не обеспечением соответствия многочисленным нормативным и ненормативным актам, заключающемся в печатании и перепечатывании бумажек, к которым всерьез никто не относится, а уменьшением реальных рисков в реальном бизнесе.

Разработка ПР способствует улучшению ситуации в области нормативного регулирования ИБ. Допустим, какая-то всеми уважаемая организация решила выпустить очередной стандарт или руководящий документ по ИБ, который как брат-близнец похож на сотню уже ранее выпущенных стандартов. Прежде, чем принять этот очередной плод нормотворчества к исполнению и начинать плодить бумажки и оценки соответствия, мы попросим авторов

предоставить ПР, обосновывающий на базе формального риск-ориентированного подхода необходимость применения данных конкретных требований к данным конкретным ИС в конкретных организациях. Если не будет ПР, тогда чем данный набор требований будет отличается от любого другого произвольным образом выбранного набора требований и какие разумные основания имеются для того, чтобы кому-то его начинать применять? Жестко формализованная структура ПР и детально проработанная методология оценки и обработки рисков, а также согласования остаточных рисков с лицами, принимающими решения, должны стать гарантиями того, что любую ерунду в ПР написать будет нельзя, т.е. конечно можно, но это будет очень заметно. Благодаря этому, плодить документы и требования по ИБ, четко не прослеживаемые до конкретных рисков конкретным информационным активам в конкретных ИС, станет невозможным.