Структура документации по управлению рисками

написано Александр Астахов | 10 июня, 2023

В мире накоплен уже значительный опыт в области управления рисками информационной безопасности. Существуют сотни книг, руководств, методик и программных продуктов. Основные требования и общие принципы управления рисками ИБ были определены в международном стандарте ISO 27001 и получили свое развитие в международном стандарте ISO 27005 и в британском стандарте BS 7799-3, представляющем собой практическое руководство по управлению рисками. Детальное описание конкретных методов оценки рисков можно найти в широко используемых на практике методологиях, таких как CRAMM, OCTAVE, RiskWatch и т.п., которые нашли свое воплощение и в соответствующих программных продуктах, позволяющих автоматизировать процессы оценки и обработки рисков. Мы рассмотрим эти и другие популярные методы и инструменты управления рисками в последней главе.

При наличии мощной теоретической и технологической базы во многих организациях до сих пор отсутствуют формализованные процессы управления рисками информационной безопасности. Такой разрыв между теорией и практикой объясняется тем, что для управления рисками недостаточно приобрести какой-либо программный инструментарий, не удастся также напрямую воспользоваться существующими методологиями и стандартами. Каждая организация, если только она не намерена передавать управление информационными рисками на аутсорсинг (идея сама по себе не лишенная здравого смысла), должна разработать и внедрить процессы управления рисками, что означает создание соответствующей организационной структуры, разработку документации, проведение обучения и осуществление контроля.

Не следует путать формализованные процессы управления рисками в организации с бюрократическими процессами, которые

отличаются избыточной формализацией и служат лишь для создания видимости какой-либо деятельности. Обычно, чем больше организация, тем ярче бывают выражены симптомы этой опасной болезни под названием бюрократизм. Внедрение любого стандарта управления, будь то ISO 27001, ISO 9001, ISO 20000 и т.п., в организации, страдающей этой болезнью в тяжелых формах, приводит лишь к дополнительным затратам собственника, появлению груды никому ненужных бумаг, дальнейшему разрастанию бюрократического аппарата и повышению нагрузки на тех немногих людей в организации, кто действительно занимается общественно полезным делом и везет на своих плечах всех остальных.

Из книги Владимира Довганя «Опыт предпринимателя»:

«Первое, что шокировало на новой работе, – отсутствие какой-либо логики в действиях администрации. К своему ужасу, я не увидел связи между текущими делами и конечным результатом, не наблюдал желания у людей обдумать абсурдную ситуацию и сделать выводы. Суть происходящего в цехе передавал афоризм, весьма популярный в коллективе: «Петров с утра бодро строит стену, зная, что после обеда Сидоров ее разрушит до основания». Команды сверху следовали одна за другой. Их невозможно было выполнить не только потому, что их было слишком много. Одни директивы нередко исключали другие. Обратной связи с верхами не было – мастера, начальники участков не могли возражать руководству цеха. Под ливнем несуразных указаний в цехе делалась масса пустой работы. Не было большей обиды для людей, чем видеть, что их труд затрачивается впустую».

«Планерки были абсолютной потерей времени. Не припомню, чтобы хоть раз разговоры на них напоминали конструктивный диалог единомышленников. Процветала «спихотехника», то есть искусство обвинять во всех бедах смежников. Это был какой-то сумасшедший дом! Самое удивительное, что большинство окружающих хорошо понимали, что участвуют в безумной игре. Но были и такие коллеги, которые уже начисто забыли, что нормальный мир

совершенно другой. Любимая пословица: «Я начальник – ты дурак, ты начальник – я дурак». Я терпел весь этот бред, надеясь пробиться наверх».

«Яркий признак иерархической, забюрократизированной структуры – уход от ответственности. Как только неудача – все пытаются свалить вину на смежников: технологи на конструкторов, конструкторы на технологов, производственники на маркетологов, маркетологи на рекламщиков, рекламщики на сбытовиков, и так до бесконечности. Никакого конструктивного подхода, логики, здравого смысла, только желание перевести стрелки на соседа. Всю жизнь одно занятие: плюнь на нижнего, толкни ближнего, подсиди верхнего. Эти патологические отношения убивают душу миллионам и миллионам людей. Иерархическая система живет ради себя. Бюрократия пожирает все вокруг. Она ведет себя как демоническое существо, чья основная задача – расти и захватывать новые горизонты».

Всем управленцам, консультантам, владельцам бизнеса и менеджерам ИБ необходимо очень хорошо различать симптомы этой опасной болезни и быть осведомленными о мерах противодействия. Если ситуация в организации напоминает описанную Владимиром Довганем в его книге «Опыт предпринимателя», тогда целесообразность внедрения СУИР вызывает сомнения.

Любая разрабатываемая для управления рисками документация должна способствовать повышению скоординированности действий всех заинтересованных лиц и повышению эффективности в достижении конечных результатов управления рисками. Следует стремиться в упрощению, избегая излишней формализации там, где без этого можно обойтись.

Ключевым моментом является разработка документации для управления рисками. Без этого дальше разговоров дело не пойдет. Только грамотно написанная документация, адекватная текущему положению дел, культуре и потребностям бизнеса

организации, позволит перейти к внедрению эффективных и измеримых процессов управления рисками.

Документацию, которая необходима для управления рисками, условно можно разделить на два уровня: нормативный и операционный. Внутренняя нормативная база организации в области управления рисками обычно представлена «Политикой управления рисками» и «Методологией оценки рисков», которые устанавливают необходимые требования и правила. Эти документы пересматриваются на регулярной основе по мере накопления организацией собственного опыта, изменения ситуации с рисками и развития бизнеса организации.

На более низком, операционном, уровне находятся рабочие документы, которые на каждодневной основе используются для отображения текущей ситуации, анализа рисков, принятия решений по обработке рисков, планирования контрмер, оценки соответствия, измерения эффективности и т.п. В число таких документов входят «Реестр информационных рисков», «Декларация о применимости», «План обработки рисков», а также таблицы, отчеты, планы, опросники, протоколы и т.п.

Структура документации, необходимая организации для управления рисками, показана на рисунке. Все эти документы вошли в состав сборника типовых документов по управлению рисками GTS 1056, который был разработан в ходе проектной деятельности GlobalTrust и послужил основой для написания настоящей книги. Подробнее об этом можно почитать в Приложении № 11.

Ниже мы подробнее расскажем о каждом из этих документов, их назначении и применении по мере того, как будем рассматривать составные элементы системы управления рисками.