Распределение ответственности за управление рисками

написано Александр Астахов | 10 июня, 2023

Почему посещая службы информационной безопасности в организациях, например, с очередным аудитом, нельзя обнаружить ни реестра информационных рисков ни плана их обработки? Ответ очевиден. Потому что эти службы не управляют рисками ИБ, а занимаются они тем, чем и должны заниматься: расследуют инциденты, управляют доступом, контролируют защищенность, фильтруют почту, борются с вредоносным ПО и т.п.

Никакого противоречия здесь нет. Все дело в том, что **задача службы ИБ состоит не в управлении рисками ИБ, а в их уменьшении до приемлемого уровня, определяемого руководством организации**.

Процесс управления рисками, как известно, включает в себя два ключевых подпроцесса: оценку и обработку рисков, а также ряд вспомогательных подпроцессов. Руководители ИБ, как можно предположить, не всегда бывают заинтересованны в экономически оправданной безопасности и объективной оценке экономического эффекта их деятельности.

Основным побудительным мотивом для вкладывания каких-либо средств в безопасность всегда являлся страх. На страхе основан и внешний и внутренний маркетинг безопасности. Размер бюджета, выделяемого на безопасность, прямо пропорционален степени обеспокоенности руководства организации этими вопросами. Чем сильнее руководителю ИБ удастся запугать свое руководство информационными угрозами, тем выше его значимость и лучше финансируется его служба.

Какие последствия для службы ИБ может иметь внедрение процесса управления рисками, при котором руководство организации будет осознанно принимать риски, опираясь на свою оценку среднегодового ущерба от инцидентов безопасности, как это

рекомендуется международными стандартами? Что если эта оценка не будет «браться с потолка», а будет определяться по прозрачной методологии, доступной для понимания и проверки всем заинтересованным сторонам, и будет опираться на мнения руководства организации, экспертов и представителей бизнеса? Вдруг такая оценка наглядно покажет, что многие затраты на безопасность не являются оправданными с экономической точки зрения? Вдруг руководство осознает и примет все риски? Что если безопасность перестанет бороться со страхами руководителей и собственников бизнеса, а вместо этого начнет работать на бизнес, помогая ему не тратить, а экономить деньги?

От таких вопросов некоторых руководителей ИБ мог бы прошибать холодный пот. Успокаивает их лишь то, что многие из них искренне не верят в возможность получения достоверных количественных оценок информационных рисков, которые были бы понятны их боссам и могли бы использоваться для принятия экономически оправданных решений.

Таким образом, за оценку рисков ИБ служба ИБ отвечать не может, потому что она не заинтересована в объективной оценке. Безопасникам выгодно, чтобы риски всегда оценивались по-максимому.

Обработка рисков включает в себя четыре взаимно-неисключающих действия: уменьшение риска, принятие (сохранение) риска, передача риска и избежание риска. Служба ИБ из всего этого может отвечать только за уменьшение риска, т.е. за планирование и реализацию конкретных контрмер.

Управление рисками – это функция более высокого уровня нежели текущая деятельность по обеспечению информационной безопасности. Она должна осуществляться руководством организации совместо с риск-менеджером, который и должен нести ответственность за формирование и поддержание в актуальном состоянии ключевых документов: реестра рисков и плана их обработки. Он также должен нести ответственность за

осуществление общего контроля процессов управления рисками, включая выполнение правил «Политики управления рисками» и обеспечение соответствия этих правил требованиям международных и национальных стандартов.

Ключевые роли по управлению информационной безопасностью в организации должны распределяться следующим образом:

- Руководство – поддержка и анализ СУИБ, утвреждение политики ИБ, распределение ключевых ролей и ответственности, определение критериев принятия рисков, общих контроль и т.п.
- Управляющий комитет по ИБ – стратегическое управление, утверждение ключевых документов и бюджета ИБ
- Служба риск-менеджмента – оценка рисков, подготовка и контроль реализации решений Руководства по обработке рисков, коммуникация и мониторинг рисков и т.п.
- Служба ИБ – оперативное управление, реализация мероприятий по обеспечению ИБ и уменьшению соответствующих рисков
- Служба внутреннего аудита – независимый контроль и оценка эффективности деятельности всех подразделений, включая риск-менеджмент, ИБ, ИТ и других участников процессов обеспечения ИБ
- Служба ИТ – реализация программно-технических механизмов контроля ИБ в зоне своей ответственности совместо или под контролем службы ИБ

Такое распределение ответственности является наиболее обоснованным, обеспечивающим взаимных контроль и исключающим конфликт интересов.

Когда руководители ИБ высказывают обоснованные сомнения в возможности реализации в рамках их подразделений процессов по управлению рисками ИБ, мы их успокаиваем: «Продолжайте заниматься текучкой, управление рисками – не ваша задача.»

В случае отсутствия в организации позиции риск-менеджера, его обязанности могут возлагаться на менеджера по информационной безопасности (CISO или директора по ИБ, т.е. на человека, отвечающего за обеспечения ИБ организации в целом), однако по приведенным выше соображениям – это не лучший вариант. Служба ИБ, также как и ИТ и бизнес-подразделения и владельцы активов должны активно участвовать в оценке рисков, но владельцем этого процесса должен быть риск-менеджер.

Служба ИБ вполне может нести ответственность за разработку, реализацию и поддержание в актуальном состоянии методологии оценки рисков информационной безопасности с учетом специфики бизнеса организации и последних достижений в предметной области.

Эффективная СУИР нуждается в извлечении информации из всех возможных источников, включая руководство, всех сотрудников и подрядчиков, безотносительно к выполняемым ими функциям, а также там, где это применимо, от внешних сторон, таких как поставщики и клиенты. Поэтому участие в процессе совершенствования СУИР должно являться частью должностных обязанностей каждого сотрудника организации.

Руководители подразделений компании должны нести ответственность за поддержку и непосредственное участие в оценке рисков информационных активов, владельцами которых они являются, а также за оценку критичности систем и конфиденциальности обрабатываемой информации.

Вице-президент (президент, генеральный или исполнительный директор) координирует выполнение корпоративной программы управления информационными рисками, утверждает «План обработки рисков» и принимает решение по допустимому уровню остаточного риска.

Ключевыми ролями в системе управления рисками являются роли риск-менеджера и эксперта по оценке рисков, которые стоит рассмотреть более подробно, опираясь на соответствующие

требования стандарта BS 7799-3.