О преимуществах системного подхода к управлению рисками

написано Александр Астахов | 10 июня, 2023

Когда пишется эта книга, мировой финансовый кризис находится в самом разгаре. Руководители и собственники организаций сейчас в основном озабочены финансовыми рисками, что не удивительно, ведь повсеместно наблюдается сокращение заказов, сворачивание проектной деятельности. Как никогда сейчас высоки кредитные и валютные риски, поскольку в финансовом мире нарушено состояние равновесия. На управление всеми прочими рисками остается значительно меньше времени и денег.

Во время финансового кризиса усиливаются не только финансовые риски, но и информационные. Массовые сокращения, урезание бюджетов и фондов оплаты труда приводят к усилению внутренней напряженности в коллективах и появлению большого количества сотрудников, недовольных своими работодателями и имеющими соответствующую мотивацию и возможности для реализации внутренних угроз в отношении информационных активов организации как самостоятельно, так и в сговоре с внешними сторонами. Такая аргументация в пользу усиления функций информационной безопасности, конечно, может оказывать определенное воздействие на руководство организации, однако все же сложно ожидать от руководства, которое и «в мирное то время» уделяло вопросам информационной безопасности явно недостаточное внимание, серьезного разворота именно в эту сторону.

Красноречие директоров информационной безопасности, методы запугивания, технологии «быстрых побед», требования законодательства и другие методы воздействия на лиц, принимающих решения, конечно, никто не отменял. Все, что срабатывало до кризиса, может сработать и сейчас. Однако не стоит питать иллюзий. В ближайшей перспективе нас ждет сокращение бюджетов и штатной численности персонала служб

информационной безопасности.

Известные аргументы в пользу усиления функции информационной безопасности, обычно предъявляемые руководству:

- *усиление внутренней угрозы во время кризиса;*
- *технология «быстрых побед»;*
- *методы запугивания;*
- *государственная «дубинка»;*
- *требования законодательства;*
- *красноречие директора по информационной безопасности и также другие способы воздействия на принятие решений.*

Все это не всегда срабатывало до кризиса, еще хуже срабатывает во время кризиса.

Исключение могут составить лишь те организации, в которых существует система управления информационными рисками. Они разительно отличаются от остальных, в которых присутствуют лишь отдельные элементы управления рисками, но нет сбалансированной системы. Различие это проявляется, прежде всего, в стабильно высоких результатах деятельности на протяжении многих лет, которые существенным образом превышают среднестатистические показатели. В таких организациях решения о финансировании информационной безопасности принимаются на основании результатов оценки рисков таким образом, чтобы максимизировать возврат инвестиций. Красноречие, магия и другие методы воздействия на руководство здесь отходят на второй план, поскольку в отлаженной системе управления технология организации работы, поставленный документооборот, а также общие цели и правила имеют куда большее значение, чем «свободное творчество» и изворотливость отдельных менеджеров информационной безопасности.

Любая система управления, выстроенная по модели Деминга, обладает большим запасом прочности, способностью к самовосстановлению и самосовершенствованию. Все элементы такой системы находятся во взаимодействии в рамках формализованных процессов и непрерывно контролируются. Если стабильность каких-то элементов нарушается, то на них немедленно оказывается корректирующее воздействие. Если какой-то элемент выходит из строя, то он легко заменяется на новый, т.к. все элементы и взаимоотношения между ними формализованы. Если даже новый элемент по своим характеристикам не тождественен старому, то ничего страшного не происходит, т.к. непрерывный мониторинг и корректировка этого элемента позволяют привести его в соответствие с целями и задачами системы.

Однако создание самоорганизующихся систем по Демингу – задача крайне непростая, требующая высокой степени профессионализма и отработанной «методы». Например, во всех организациях есть продавцы, но далеко не каждая может похвастаться наличием эффективной системы продаж, как у лидеров рынка. Любая система продаж строится из трех основных элементов:

- особым образом отобранные и подготовленные кадры;
- технологии и стандарты продаж, включая внутренний документооборот отдела продаж;
- процесс управления отделом продаж, реализуемый его руководителем, и конкретные обязанности этого руководителя и его сотрудников.

Если в чем-то из перечисленного существует «прокол», то продажи не идут.

Во многих организациях управляют проектами, но лишь в немногих существует эффективная система управления проектами, которая строится из тех же трех элементов, что и система продаж. Такие организации способны меньшими силами выполнять значительно большее количество более сложных проектов, при этом обходясь без эксцессов.

Многие российские производственные компании отличаются от западных прежде всего тем, что в первых есть только определенные элементы контроля качества, а в последних существует эффективная система контроля качества, выстроенная по модели Деминга. Отсюда такая разница в производимой продукции и вытекающие отсюда конкурентные преимущества.

Такие же наблюдения характерны и для моделей управления рисками и безопасностью, применяемых в организациях. Наш опыт внедрения и сертификации систем управления информационной безопасностью организаций (а это довольно успешные по российским меркам организации) по требованиям международного стандарта ISO 27001, а также опыт проведения аудита таких систем показывают, что практически во всех организациях можно найти отдельные механизмы контроля, описанные в стандарте, однако отсутствует фундамент, объединяющий эти механизмы в систему, позволяющую получать гарантированный, стабильный и измеримый результат. Для информационной безопасности таким результатом является сокращение среднегодовых потерь и повышение возврата инвестиций в безопасность без ущерба для интересов бизнеса.

Фундаментом СУИБ служит система управления информационными рисками, представляющая собой:

1. совокупность взаимосвязанных формализованных процессов, обеспечивающих анализ и планирование, реализацию и эксплуатацию, мониторинг и аудит, корректировку и совершенствование механизмов управления рисками;
2. стандарты и технологии управления рисками, представленные в виде нормативной и рабочей документации СУИР, включающей в себя политику управления рисками и методологию оценки рисков, а также еще около 20 рабочих документов, из которых самыми важными являются Реестр информационных рисков и План обработки рисков;
3. организационную структуру управления рисками и соответствующим образом подготовленный персонал. Роли и

ответственность за функционирование процессов управления рисками распределяются между руководством организации, управляющим комитетом по информационной безопасности, рабочей группой по оценке рисков, владельцами активов, пользователями и обслуживающим персоналом информационных систем, менеджером информационной безопасности, риск-менеджером и аудиторами.

Практика внедрения и сертификации СУИБ самых разных компаний показывает, что оценка рисков – это «ахиллесова пята» современных организаций, обычно вызывающая наибольшие затруднения. Во многих случаях ситуация такова, что руководство организации не располагает необходимой и своевременной информацией о рисках информационной безопасности для принятия адекватных решений в этой области, контроля реализации и оценки эффективности принятых решений. Во многих организациях отсутствуют система сбора и анализа информации об информационных рисках, механизмы обработки и пересмотра рисков, механизмы коммуникации рисков и другие необходимые элементы, без которых система управления рисками не работает.

Три необходимых составляющих СУИР:

- *формализованные взаимодействующие процессы;*
- *стандарты, технологии, внутренний документооборот;*
- *организационная структура и кадры.*

Не может СУИР функционировать и без четко определенных и согласованных со всеми участниками процесса критериев оценки и принятия рисков, области оценки и других элементов, определяемых политикой управления рисками.

Не стоит также забывать и о целях управления рисками, способах

оценки достижения этих целей, методах измерения эффективности механизмов контроля и системе поощрения персонала, которая должна быть связана с достижением целей СУИР и эффективностью реализуемых механизмов контроля. У многих ли менеджеров информационной безопасности и риск-менеджеров в наши дни зарплата зависит от достижения целей управления рисками и возврата инвестиций? Чем тогда эти менеджеры мотивированы на достижение результатов? Ведь, как известно, материальное стимулирование является одним из основных способов мотивирования персонала.

Разработка и внедрение СУИР – процесс достаточно трудоемкий, требующий высокого профессионализма и большого опыта в управлении рисками. Теоретически каждая организация, начинающая осознавать свои потребности в обеспечении информационной безопасности, в состоянии двигаться по пути создания СУИР самостоятельно, однако на практике многие заходят в тупик на этом пути. Это происходит не только из-за недостатка опыта, профессиональной квалификации и глубины осознания информационных рисков.

Дело в том, что внедрение СУИР зачастую связано с весьма существенными изменениями существующей системы управления организацией и пересмотром принятых подходов к принятию решений. Это особенно сложно сделать, если в организации до сих пор вообще отсутствовала какая-либо система управления рисками (ERM-система) и соответствующих элементов такой системы просто не существует. В этом случае изменить систему управления изнутри крайне сложно. Ведь любая система стремится к стабильности и сохранению своего прежнего состояния.

Поэтому во многих случаях помощь со стороны внешних консультантов, имеющих достаточный опыт внедрения СУИР и владеющих соответствующими технологиями, является оправданной. Опытные консультанты смогут провести обучение персонала, формализовать процессы и разработать систему внутренней документации для управления рисками, провести первоначальную оценку рисков и разобраться с проблемами, которые возникнут по

ходу этой оценки, а также «подтолкнуть» руководство организации с целью скорейшего рассмотрения и принятия решений по рискам.

Для организаций, в которых информационные риски не являются основными, существует вариант отдачи процесса управления рисками на аутсорсинг специализированной организации. Теоретически аутсорсинг должен обеспечить сокращение затрат при сохранении достаточного уровня контроля над процессами управления рисками.