О чем эта книга?

написано Александр Астахов | 10 июня, 2023

Эта книга подытоживает многолетний практический опыт автора в области управления информационными рисками. Этот опыт нашел отражение в методологии и продуктах компании GlobalTrust, которые успешно применяются в ряде российских организаций.

Автор полагает, что наш подход к управлению рисками, вообще говоря, является достаточно универсальным и успешно может применяться для управления любыми физическими и операционными рисками, а также, возможно, и любыми неспекулятивными рисками, т.е. теми рисками, единственными последствиями которых, является причинение ущерба организации. Британский стандарт BS 31100 раскрывает именно эту тему. Ведь для любых неспекулятивных рисков факторы риска (такие как угрозы, уязвимости, активы и контрмеры) и подходы к их анализу остаются неизменными. Меняется лишь область экспертной оценки. Однако существует множество нюансов, которые мы здесь не в состоянии учесть, поэтому будем оставаться в рамках своей предметной области и, чтобы не усложнять и без того непростую тему, при дальнейшем изложении под рисками будем понимать исключительно риски информационной безопасности.

Об управлении рисками на разных языках написано довольно много научных и околонаучных трудов, изобилующих математическими формулами, моделями, принципами, количественными и качественными подходами, теориями полезности, субъективной вероятности, непрерывными распределениями, нечеткими множествами и прочими теориями, не имеющими прямого отношения к реальной жизни. Птичий язык многих из этих сочинений, оторванность от практики, отсутствие параллелей с теми обстоятельствами, в которых вынужден функционировать современный бизнес, приводит к тому, что их аудитория ограничивается очень узким кругом специалистов, по большей части теоретиков, имеющих узкоспециальное образование и владеющих соответствующим математическим аппаратом, в то время

как оценка рисков имеет очень мало общего с математикой вообще. Для широкой аудитории вопросы управления информационными рисками остаются практически неведомыми.

Если финансовая безграмотность сегодня приводит к плачевным результатам, то информационная безграмотность способна породить еще худшие результаты уже в недалеком будущем. В наше время, управление рисками – это отнюдь не какая-то математическая теория, имеющая прикладное значение. Управление рисками – это жизненная необходимость для все большего числа организаций. Кого-то эти проблемы еще не коснулись в достаточной степени, для кого-то это вопрос эффективности управления бизнесом, а для других это уже вопрос выживания. Мы постарались избавиться от всей псевдонаучной шелухи, заслоняющей важнейшие вопросы, связанные с управлением информационными рисками, и сосредоточиться только на тех идеях, которые обладают свойством практической полезности, попытавшись изложить свой подход простым человеческим языком.

Автор надеется, что эта книга поможет читателю без особых проблем перейти к систематическому управлению рисками в соответствии с международными стандартами, используя простой и прагматичный подход, неоднократно проверенный на практике и основанный на доступном каждому человеку здравом смысле.

Если послушать, что говорят, и почитать, что пишут об управлении рисками, то может сложиться впечатление, что задача эта чрезмерно сложная и трудоемкая, что этот вопрос лежит, скорее, в теоретической плоскости, а на практике целесообразно применять более простые подходы к выбору защитных мер. Эти рассуждения, на наш взгляд, сильно преувеличены. Для адекватной оценки риска не требуется ни учености, ни шаманства. Каждый специалист, имеющий достаточный опыт работы в области информационной безопасности, может овладеть этим нехитрым ремеслом. Правда, ему для этого придется переориентироваться на бизнес и научиться осуществлять декомпозицию бизнес-целей и процессов до поддерживающих их информационных активов и связанных с ними угроз и уязвимостей,

а уже от них переходить к механизмам безопасности, которыми он привык заниматься. Здесь, скорее, потребуются не новые знания, а перенастройка мышления с технически ориентированного на бизнес-ориентированное и риск-ориентированное.

Тем же, кто не является специалистом в области информационной безопасности или информационных технологий, эта книга поможет осознать сущность проблем информационной безопасности, а также то, каким образом информационные риски влияют на них лично, на организацию, в которой они работают, на их бизнес, а также на общество, в котором они живут. Это позволит подготовиться к ближайшему будущему, переполненному информацией и связанными с этим рисками, а также к новым информационным кризисам, которые могут прийти на смену финансовым.