СОДЕРЖАНИЕ

Нью-Йоркская фондовая биржа с их Уолл Стритом и трейдерами, с выпученными глазами выкрикивающими котировки акций в переполненном зале, скоро станет анахронизмом и будет заменена электронными торговыми площадками и молодыми ребятами с ноутбуками, проворно перетаскивающими миллионы долларов между виртуальными счетами за считанные секунды, не отрываясь от кружки пива в любимом клубе, а может быть, лежа на диване, — совершенно неважно, в какой стране мира он в данный момент находится. В современном обществе тем, кто не успевает освоиться с информационными технологиями и адаптироваться к новым правилам игры, достается самая тяжелая и низкооплачиваемая работа.

Когда все более или менее значимые для людей процессы окажутся полностью компьютеризированными, а финансовые и информационные системы глобализированными (а это фактически уже почти что произошло в развитых странах), на первое место выйдут информационные риски. Министр информационной безопасности, возможно, станет не менее значимой для государства фигурой, нежели министр обороны или министр финансов. Этим «фантазиям» суждено сбыться, возможно, уже в грядущем десятилетии — раньше, чем многие успеют осознать, что же произошло.

О чем эта книга?

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, то есть 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,

ность 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.

Существуют ли альтернативы управлению рисками?

Альтернативы управлению рисками, на наш взгляд, сегодня уже не существует. Информационная безопасность не относится к числу проблем, которые можно решать по мере их возникновения. Либо вы управляете рисками, либо риски управляют вами. Проактивный подход намного лучше реактивного. Когда возникает проблема с безопасностью, часто бывает уже слишком поздно ею заниматься. Поэтому надо заранее анализировать и упреждать возможные проблемы, руководствуясь при этом соображениями экономической целесообразности.

Правила игры стремительно меняются. Сегодня уже недостаточно просто реагировать на появление новых угроз, руководствоваться при выборе защитных мер общими соображениями и укоренившимися взглядами на информационную безопасность как на какое-то мало значимое побочное явление, сопутствующее внедрению информационных технологий и ассоциирующееся в массовом сознании с понятиями «хакер» и «компьютерный вирус», находящимися где-то там, далеко от нас. Информационная безопасность — это уже не отдельно взятые угрозы, обязанные своим распространением главным образом сети Интернет, а новая система взаимоотношений в изменившемся мире, где уже не действуют прежние законы.

Без управления рисками все еще, как и раньше, можно достигать определенных положительных результатов, однако стабильных результатов достигать все сложнее. Поэтому компании, систематически управляющие рисками, по крайней мере, обладают важнейшим конкурентным преимуществом.

Пока происходило (и до сих пор происходит) столь бурное, порой революционное во многих областях, освоение новых технологий, основной лозунг звучит просто: «лишь бы все заработало». Когда же все это наконец начинает работать, да так, что остановить это уже невозможно, то на первый план выходит соображение «не дай бог это вдруг остановится или сработает не так, как планировалось», то есть на первый план выходят соображения безопасности, и уже ИТ занимает по отношению к ним подчиненное положение. С того момента, как останов информационных систем начинает приводить к катастрофическим последствиям, становится совершенно необходимым управлять информационными рисками на систематической основе, соотнося расходы на защиту с получаемой выгодой.

Насколько глобальными могут быть последствия недооценки рисков, возникающих в связи с изменением мироустройства, мы с вами имеем возможность наблюдать сегодня на примере захлестнувшего весь цивилизованный мир финансового кризиса, основной причиной которого является отсутствие адекватного управления финансовыми рисками, а порой и самого осознания этих рисков, не только среди обывателей, но и среди профессионалов.

Почему управление рисками является самым важным вопросом информационной безопасности?

Чтобы разобраться с любой проблемой безопасности, необходимо ответить на четыре вопроса: «Что?», «Почему?», «От чего?» и «Как защищать?». Оценка рисков позволяет разобраться с первыми тремя вопросами, а обработка риска — связать первые три вопроса с последним вопросом «Как?». Все остальные знания в области безопасности посвящены лишь ответу на вопрос «Как защищаться от тех или иных конкретных угроз?». Однако отвечать на этот вопрос бессмысленно, не разобравшись в первыми тремя вопросами. Этим объясняется первичность темы управления рисками и ее приоритет над всеми остальными вопросами.

Поэтому при разработке мастер-класса, материалы которого послужили прототипом для написания настоящей книги (см. Приложение № 15), мы сделали его достаточно дорогим, с целью отсечь ту часть аудитории, которая приходит на подобные мероприятия в основном для того, чтобы просто пообщаться, отдохнуть от основной работы и заодно немного расширить свой кругозор. Нам хотелось, чтобы на нашем мероприятии присутствовали только те люди, для которых управление рисками является уже осознанной необходимостью и которые готовы инвестировать и время и деньги в обучение этому вопросу.

Автор надеется, что после прочтения этой книги управление рисками станет осознанной необходимостью и для вас.

Для кого написана эта книга?

Эта книга рассчитана на широкую аудиторию просвещенных людей, интересующихся вопросами управления информационными рисками в стремительно меняющемся информационном веке, в котором не действуют привычные стереотипы, не работают старые правила, подвергаются пересмотру экономические законы, принципы ведения бизнеса и человеческие ценности, а информация превращается в один из главных и наиболее уязвимых активов.

Безусловно, в первую очередь данный материал должен заинтересовать специалистов по информационной безопасности, включая менеджеров, аудиторов, экспертов, аналитиков, инженеров, а также всех тех, кто:

- принимает решения по информационной безопасности и ее финансированию;
- имеет отношение к оценке и управлению информационными рисками в организации;
- участвует в планировании и проведении аудитов информационной безопасности;
- осуществляет планирование мероприятий по информационной безопасности и расставляет приоритеты;
- формирует и обосновывает бюджет на информационную безопасность;
- оценивает экономическую эффективность и целесообразность реализации защитных мероприятий;
- внедряет системы управления информационной безопасностью и/или готовит организацию к сертификации по требованиям международного стандарта ISO 27001.

Автор также надеется, что эта книга окажется интересной и полезной для значительно более широкой аудитории, включая специалистов в области информационных технологий различных профилей, руководителей бизнеса, риск-менеджеров, а также для всех тех, кто желает:

- взять под контроль риски информационной безопасности во всех сферах деятельности;
- расширить и углубить свое понимание сущности процессов обеспечения информационной безопасности;
- перейти от общих рассуждений о связи бизнеса, информационных технологий и безопасности к реальным действиям по управлению этими взаимосвязями;
- взглянуть на проблемы безопасности с точки зрения бизнеса и, наоборот, оценить надежность и жизнеспособность бизнеса с точки зрения защищенности его информационных активов.

Общая структура изложения материала

Эта книга помимо предисловия, введения, заключения и приложений включает в себя шесть глав.

Структура книги:

- Глава 1. Предпосылки для управления информационными рисками
- Глава 2. Основные элементы управления информационными рисками
- Глава 3. Система управления информационными рисками
- Глава 4. Оценка рисков информационной безопасности
- Глава 5. Обработка рисков информационной безопасности

- Глава 6. Инструментальные средства для управления информационными рисками
- Вместо заключения – практические советы по внедрению системы управления рисками
- Приложения

Первая глава отвечает на вопрос первостепенной важности, без утвердительного ответа на который, возможно, и не стоило бы писать эту книгу: «Почему в наше время крайне важно управлять информационными рисками, а в недалеком будущем по причине недооценки информационных рисков человечество ожидают информационные кризисы, пострашнее нынешнего мирового финансового кризиса?» В первой главе книги мы попытаемся проложить дорогу между настоящим и будущим, показывая, почему уже сейчас многие организации не могут обойтись без систематического управления рисками, почему сегодня нельзя относиться к управлению рисками, руководствуясь вчерашними представлениями, и почему завтра ситуация с информационными рисками может измениться кардинальным образом, что станет неожиданностью для многих людей, не успевших адаптироваться к стремительно изменяющимся обстоятельствам.

Во второй главе, опираясь на международные стандарты, мы дадим несколько равнозначных определений понятию «информационный риск», рассмотрим основные составляющие этого непростого понятия, факторы (элементы) риска, рассмотрим, чем обусловлено различие подходов к оценке рисков, применяемых в организациях. Мы также коснемся количественных и качественных способов определения величины риска, а заодно развеем распространенное заблуждение и покажем, что, несмотря на разнообразие способов вычисления рисков, не существует самодостаточных количественных или качественных подходов к оценке рисков, которые могли бы иметь прикладное значение, а в сущности, на практике имеет место комбинированный подход.

Как показывает опыт внедрения систем управления информационной безопасностью (СУИБ) в российских организациях и опыт их сертификации по требованиям международного стандарта ISO 27001, главной точкой преткновения обычно становится система управления рисками. В третьей главе мы рассмотрим эту систему, служащую базисом для СУИБ, в комплексе, опираясь на определяемую стандартами процессную модель. Если взглянуть на проблему широко, то мы увидим, что она не сводится лишь к двум ключевым процессам оценки и обработки риска. Для того чтобы система управления рисками оставалась жизнеспособной и могла адаптироваться к изменяющимся условиям, она должна включать в себя еще целый ряд процессов, обеспечивающих непрерывный контроль и совершенствование этой системы и теснейшим образом интегрированных со всеми остальными процессами СУИБ.

Четвертая глава является ключевой с точки зрения понимания используемой нами методологии оценки рисков. В ней шаг за шагом рассматриваются

все стадии этого процесса, начиная с инвентаризации активов и заканчивая формированием реестра информационных рисков. При этом мы не раскрываем каких-то секретов и в сущности не сообщаем каких-то сведений, которые сами по себе уже не были бы известны специалистам и не были бы описаны в стандартах. Мы склонны видеть свою заслугу, если мы вообще вправе на это претендовать, не в передаче некоего тайного знания, а скорее, в систематизации накопленного опыта и знаний профессионального сообщества, а также в переводе вопросов, которые обычно вызывают серьезные затруднения у многих специалистов, в практическую плоскость, разрешая их просто, сообразно сложившимся обстоятельствам и без излишнего теоретизирования.

Не так важно, какой подход к оценке рисков вы используете, а мы отнюдь не считаем, что наш подход является единственно возможным, главное — насколько адекватные и экономически оправданные решения по обработке рисков вы в конечном счете принимаете. В пятой главе книги мы рассмотрим возможные способы обработки рисков, механизмы планирования защитных мер и принятия решений по рискам, а также вопросы оценки возврата инвестиций в информационную безопасность. Основным результатом данных мероприятий служит разработка двух ключевых для СУИБ документов: Декларации о применимости механизмов контроля и Плана обработки рисков.

Шестая глава посвящена обзору наиболее популярных инструментальных средств управления рисками. Помимо этого мы рассмотрим проблему выбора специализированного программного инструментария для оценки рисков с различных точек зрения, а также плюсы и минусы, связанные с его использованием. Вопрос практической целесообразности применения подобного инструментария в конкретной ситуации мы оставим на усмотрение читателя.

В Заключении приводится ряд практических советов по внедрению системы управления информационными рисками, начиная с необходимых предпосылок для управления рисками, разработки документации, формирования организационной структуры, проведения пилотного проекта и заканчивая полной оценкой рисков и поддержкой жизненного цикла процессов управления рисками.

В конце каждой главы приведен список несложных вопросов, над которыми рекомендуется самостоятельно поразмыслить, прежде чем переходить к чтению следующей. По ходу изложения материала предусмотрено также несколько практических заданий, которые мы выполняем на мастер-классе по управлению рисками, чтобы сохранить бодрость ума для лучшего восприятия материала и закрепить полученные знания. Читателю мы предлагаем не лениться и последовать нашему примеру, так как, несмотря на все усилия автора, материал книги местами достаточно абстрактен и требует для своего восприятия свежего и подготовленного ума.

Информация справочного характера вынесена в Приложения. Там же вы найдете информацию о компании GlobalTrust, реализуемых нами продуктах и услугах, а также о том, каким образом эти продукты и услуги могут помочь вам в решении вопросов управления информационной безопасностью и рисками.