СОДЕРЖАНИЕ

ОБ АВТОРЕ

Александр Астахов — эксперт по информационной безопасности с 14-летним опытом работы в предметной области, реализовавший десятки комплексных проектов по созданию систем защиты информации в компаниях различного масштаба и сферы деятельности, широко известный своими публикациями в прессе.

Александр является учредителем и генеральным директором компании ГлобалТраст (GlobalTrust, http://www.globaltrust.ru), одного из технологических лидеров российского рынка систем управления информационной безопасностью, разрабатывающего уникальные для России информационные продукты и методики по управлению безопасностью и рисками. ГлобалТраст — одна из первых российских компаний, реализующих проекты по внедрению и сертификации систем управления информационной безопасностью в соответствии с требованиями международного стандарта ISO 27001, начиная с 2005 года.

Александр родился в 1972 году. Окончил Институт криптографии, связи и информатики Академии ФСБ России в 1995 году и адъюнктуру в 1998 году. До 2000 года занимался преподаванием на кафедре программирования и компьютерной безопасности, затем работал в коммерческих компаниях, за несколько лет пройдя путь от ведущего специалиста до руководителя направления информационной безопасности в ряде российских системных интеграторов. Довелось также поработать и «на другой стороне баррикад» в качестве аудитора и начальника отделов информационной безопасности в финансовом и промышленном секторах.

В 2003 третьем году основал компанию ГлобалТраст, которая должна была компенсировать отсутствие на российском рынке в то время качественных услуг и инструментов для управления информационной безопасностью. Основными проектами ГлобалТраст являются: консалтинг и обучение, создание новых продуктов для управления безопасностью и рисками, дистрибуция лучших мировых брендов, развитие интернет-магазина средств защиты информации shop.globaltrust.ru и информационного портала ISO27000.RU — авторитетного русскоязычного ресурса, посвященного вопросам управления безопасностью и рисками, который ориентирован на новое поколение менед-

жеров информационной безопасности, способных управлять взаимосвязями между бизнесом, безопасностью и информационными технологиями.

Александр – ведущий преподаватель Британского Института Стандартов (BSI, http://www.bsi-global.com), сертифицированный аудитор информационных систем (CISA) с 2000 года, автор учебных курсов по аудиту, управлению рисками и внедрению систем управления информационной безопасностью, главный редактор лицензионных русских переводов международных и британских стандартов в области защиты информации и управления непрерывностью бизнеса.

С Александром Астаховым можно связаться по электронной почте AlexAstahov@globaltrust.ru.

Его блог находится по адресу: http://www.iso27000.ru/blogi/alexandr-astahov.

ПРЕДИСЛОВИЕ

Книга Александра Астахова «Искусство управления информационными рисками» предоставляет читателям возможность познакомиться с основами управления рисками информационной безопасности, а также с шагами, необходимыми для быстрого и успешного перехода от разговоров об искусстве, сложности и нетривиальности задачи управления информационными рисками к простой и эффективной практике оценки, анализа и обработки рисков.

Любой специалист, занятый в сфере построения и управления системой менеджмента информационной безопасности, а также подготовкой ее к возможной сертификации (регистрации) на соответствие требованиями стандарта ISO 27001, сочтет эту книгу полезной и поучительной.

В книге читатель получит подробную инструкцию по организации процессного подхода управления рисками, найдет информацию об инструментах автоматизирующих этот процесс, освоит базовые определения и концепции, начиная с угроз и уязвимостей, и, заканчивая вопросами приемлемых уровней рисков, их обработки и принятия, превентивными и корректирующими действиями.

Последовательное изложение, формат, обеспечивающий легкое и интересное чтение, практический опыт автора и система взглядов, изложенная в международных стандартах серии ISO 2700x, все это позволяет надеяться, что книга может служить хорошим инструментом в повседневной работе специалистов, управляющих рисками информационной безопасности.

Александр Невский, CISA, CISSP
Начальник управления информационной безопасности
КБ «Ренессанс Капитал» (ООО)

ПРЕДИСЛОВИЕ АВТОРА

Эта книга поможет профессионалу систематизировать имеющиеся знания и перейти к созданию эффективной системы управления рисками, соответствующей потребностям его организации. Новичку же она даст базовый набор знаний, необходимый для того, чтобы обеспечить ему хороший старт в области управления рисками.

Управление информационными рисками — тема для многих неочевидная, значение которой в жизни общества неуклонно возрастает. В скором времени она может выйти на первый план, наряду с политическими, финансовыми и военными событиями. Поэтому политикам, бизнесменам, военным, руководителям всех уровней, а также всем специалистам, имеющим какое-либо отношение к информационным технологиям, важно подготовить свое сознание к восприятию новой реальности и решению невиданных ранее проблем, связанных с возрастанием угроз информационной безопасности.

Однако в первую очередь эта книга адресована специалистам по информационной безопасности, которых совсем недавно начали готовить в университетах в соответствии с «лучшими традициями» высшего образования, то есть далеко от реальной жизни. Большая же часть практикующих специалистов по информационной безопасности пришло в эту область из информационных технологий, унаследовав технический взгляд на безопасность, соответствующий менталитет и самоощущение «чужого среди своих». И тем и другим предстоит пройти долгий путь с целью обретения гармонии в такой сложной области, как информационная безопасность.

Эта странная область деятельности, ассоциирующаяся в массовом сознании с хакерами и компьютерными вирусами, а в наше время еще и с утечками данных, находится на стыке информационных технологий, безопасности, общего менеджмента и психологии. Для успешного решения проблем информационной безопасности требуются нетрадиционные подходы, а также совмещение знаний и навыков из различных технических и гуманитарных областей, которые сложно совместить в одном человеке. А упираются все эти непростые вопросы в конечном счете в управление рисками.

Автор будет считать свою задачу выполненной, если его многолетний опыт, приобретенный в пока еще слабо защищенном от информационных угроз российском бизнесе, окажется полезен читателям и будет способствовать укреплению безопасности и стабильности общества, повышению эффективности менеджмента и просветлению в умах.

У просвещенного читателя эта книга, возможно, вызовет даже больше вопросов, нежели сможет дать ответов. Безусловно, какие-то темы в ней остались раскрыты недостаточно глубоко. Не стоит питать иллюзий на этот счет. Нельзя объять необъятного. Не стоит упрекать автора в том, что он ответил не на все вопросы и раскрыл не все «профессиональные тайны». Тем более, что основной секрет управления рисками заключается в отсутствии каких-либо секретов. Вместо «профессиональных тайн» автор предлагает систематический подход, основанный на здравом смысле, международных стандартах и обобщении практического опыта, накопленного в этой сфере профессиональным сообществом.

Автор не ставил перед собой цели в рамках одной книги дать ответы на все вопросы, раз и навсегда решив все проблемы, возникающие при управлении рисками. Слишком сложна и многогранна эта тема для того, чтобы ее можно было так скоро исчерпать. Поэтому автор с благодарностью и вниманием воспримет любые конструктивные замечания и предложения по улучшению и дополнению сего труда, отправленные читателями на его электронный адрес: alexastahov@globaltrust.ru.

ВВЕДЕНИЕ

- Новые правила игры в новом информационном веке.
- О чем эта книга?
- Существуют ли альтернативы управлению рисками?
- Почему управление рисками является самым важным вопросом информационной безопасности?
- Для кого написана эта книга?
- Общая структура изложения материала.

Эта книга опирается на сегодняшний опыт, но ее основная стратегическая задача — подготовить вас к восприятию новой реальности в значительной степени изменившегося мироустройства, которая наступит уже после глобального финансового кризиса, когда неожиданно для многих на смену финансовым проблемам придут проблемы информационные.

Новые правила игры в новом информационном веке

Переход через условный рубеж 2000 года ознаменовал собой переход от индустриального века к информационному — поворотный момент в истории человечества, не осознанный еще в полной мере. Знаменитая «проблема» 2000 года и поднятая вокруг этого шумиха только обозначили этот переход и, хотя тема была в основном «раздута» и под это дело, так уж повелось, было «отмыто» немало «бабок», акцент поставлен правильный — благосостояние, а вероятно, и выживание будущих поколений постепенно окажется в зависимости от информационных технологий и связанных с ними рисков информационной безопасности.

В новом веке ситуация во всем мире начала изменяться еще быстрее, чем раньше: невиданные по своей дикости терракты, гибель крупнейших корпораций, невиданный доселе экономический кризис у лидеров мировой экономической системы США и Японии, который пока только усугубляется и тащит за собой к финансовому краху Европу и все остальные страны, интегрированные в мировую финансовую систему.

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,

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 сущ-

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