
Обеспечение
информационной
безопасности бизнеса
под редакцией А.П. Курило
IBM

В. В. Андрианов

Обеспечение информационной безопасности бизнеса

«Центр Исследований Платежных Систем и Расчетов»

2010

Андрианов В. В.

Обеспечение информационной безопасности бизнеса /
В. В. Андрианов — «Центр Исследований Платежных Систем и Расчетов», 2010

Данную книгу можно назвать практической энциклопедией. В ней дан максимальный охват проблематики обеспечения информационной безопасности, начиная с современных подходов, обзора нормативного обеспечения в мире и в России и заканчивая рассмотрением конкретных направлений обеспечения информационной безопасности (обеспечение ИБ периметра, противодействие атакам, мониторинг ИБ, виртуальные частные сети и многие другие), конкретных аппаратно-программных решений в данной области. Книга будет полезна бизнес-руководителям компаний и тем, в чью компетенцию входит решение технических вопросов обеспечения информационной безопасности.2-е издание, переработанное и дополненное

Содержание

В.В. Андрианов, С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев Обеспечение информационной безопасности бизнеса Под общей редакцией А.П. Курило

Предисловие А.А. Стрельцова

Среди множества проблем социально-экономического развития России в условиях формирования глобального постиндустриального общества заметное место занимает организация устойчивого функционирования и безопасности использования информационных систем и информационно-коммуникационных сетей, обеспечивающих экономическую деятельность. По мере усложнения информационной инфраструктуры бизнеса влияние данного фактора на результаты деятельности коммерческих организаций будет возрастать. Это наглядно видно на примере развития экономики США, для которых обеспечение компьютерной безопасности стало одним из национальных приоритетов XXI в.

Проблема обеспечения информационной безопасности бизнеса имеет много аспектов, но все они так или иначе объединены необходимостью стандартизации принимаемых решений – своеобразной платой за преодоление «проклятия размерности», порождаемого сложностью управляемых процессов.

Предлагаемая вниманию читателей книга «Обеспечение информационной безопасности бизнеса» посвящена рассмотрению стандартов обеспечения информационной безопасности коммерческой организации, представляющей собой основного субъекта экономики общества. В данном случае стандарты – это прежде всего система правил поведения лиц, участвующих в принятии и реализации решений по построению системы обеспечения информационной безопасности организации. С этой точки зрения стандарты являются важным элементом культуры постиндустриального общества, оказывающей непосредственное влияние на эффективность экономической деятельности не только организации, но и общества в целом. Установление стандартов поведения и следование им – важный показатель социальной зрелости общества и общей культуры его членов. Стандарты являются той основой культуры массового производства и потребления, без которой расширение специализации в осуществлении производственной деятельности и потребления ее продуктов, на которых наряду с частной инициативой базируется глобальная экономика мира, было бы невозможным.

Как показывает опыт, одной из наиболее сложных проблем обеспечения информационной безопасности является объяснение руководителю организации в доходчивой форме, чем именно занимается коллектив специалистов по информационной безопасности, почему на эту работу нужно тратить значительные финансовые и иные ресурсы, чего именно можно ожидать в результате этих затрат и как он лично может убедиться в том, что выделенные ресурсы не потрачены впустую. Подобные вопросы возникают не только на уровне руководства организации, но и на уровне многих руководителей федерального, регионального и местного масштаба. Предлагаемая вниманию читателей книга делает существенный шаг вперед в поиске ответов на эти вопросы.

Книга подготовлена авторским коллективом, члены которого обладают большим опытом практической работы по решению сложных проблем обеспечения информационной безопасности в различных сферах экономической деятельности.

Авторы предприняли попытку поставить и решить задачу развития стандартов обеспечения информационной безопасности применительно к деятельности коммерческой организации, увязать связанные с этим вопросы с бизнес-процессами, которые для любой коммерческой организации являются приоритетными. Предлагаемый авторами подход к стандартизации процессов обеспечения информационной безопасности организации базируется на результатах философского осмысления проблемы, ее сущности, а кроме того, на возможных проявлениях в реальной жизни и на разработке структурированных описаний (схем-моделей) стандартизируемых процессов.

Структурно работа состоит из четырех разделов основного материала и приложений.

В первом разделе на основе изучения роли и места информации в бизнес-процессах, а также анализа видов информации, в которых данные процессы проявляются (учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы и т. п.), разработана обобщенная схема – модель информационной безопасности бизнеса. Данная модель основана на анализе источников возникновения рисков снижения эффективности бизнеса, возникающих в информационной сфере организации.

На основе анализа известных схем – моделей осуществления менеджмента разработана схема – модель управления процессами обеспечения информационной безопасности организации или управления рисками нарушения ее информационной безопасности. Данная схема представлена во втором разделе. С учетом устоявшегося подхода к унификации описаний процессов менеджмента предложено стандартизованное описание системы менеджмента информационной безопасности организации, а также реализации ее отдельных составляющих (менеджмента рисков, инцидентов, активов, документов и т. п.).

Возможные методики оценки уровня информационной безопасности организации и примеры их использования рассмотрены в третьем разделе.

В четвертом разделе основное внимание сосредоточено на исследовании проблем противодействия «внутренним» угрозам информационной безопасности, исходящим от сотрудников организации. Предложена соответствующая модель угроз и рассмотрены возможные меры по противодействию этим угрозам.

В приложении приведены справочные материалы по архитектуре стандартов защиты информации и обеспечения информационной безопасности и др., а также изложены подходы к формированию нормативного обеспечения системы информационной безопасности организации.

Практическая значимость книги заключается в том, что в ней с единых методологических позиций рассмотрены проблемы формирования системы обеспечения информационной безопасности организации как упорядоченной совокупности нормативных, организационных и технических решений, позволяющих не только обеспечить противодействие угрозам нарушения информационной безопасности, но и повысить прозрачность процесса построения и функционирования таких систем.

Предложенные в книге выводы и рекомендации базируются на анализе конкретных нормативных и методических материалов, подкрепляются наглядными иллюстрациями и обладают значительным потенциалом дальнейшего развития.

Материалы книги будут полезны ученым и специалистам, занимающимся вопросами обеспечения информационной безопасности организаций, а также студентам, изучающим соответствующие учебные курсы.

А. А. Стрельцов,

профессор, заслуженный деятель науки Российской Федерации, доктор технических наук, доктор юридических наук

Предисловие С. П. Расторгуева

Проблема обеспечения информационной безопасности – вечная проблема, и она будет вечной до тех пор, пока под безопасностью мы будем понимать состояние или ощущение защищенности интересов (целей) организации в условиях угроз. Почему? Потому что состояние защищенности – это субъективное понятие. У волка оно одно, а у овцы – совсем другое. В случае же человека или социума все еще гораздо сложнее, и в общем случае никогда нельзя сказать, чем все это дело закончится, как в известной даосской притче про старика (http://pritchi.castle.by/ras-14-1.html): «Жил в одной деревне старик. Был он очень беден, но все императоры завидовали ему, потому что у него был прекрасный белый конь. Никто никогда не видел подобного коня, отличавшегося красотой, статью, силой… Ах, что за чудо был этот конь! И императоры предлагали хозяину за коня все, что только бы он пожелал! Но старик говорил: “Этот конь для меня не конь, он – личность, а как можно продать, скажите на милость, личность? Он – друг мне, а не собственность. Как же можно продать друга?! Невозможно!” И хотя бедность его не знала пределов, а соблазнов продать коня было немыслимое количество, он не делал этого.

И вот однажды утром, зайдя в стойло, он не обнаружил там коня. И собралась вся деревня, и все сказали хором: “Ты – глупец! Да мы все заранее знали, что в один прекрасный день этого коня украдут! При твоей-то бедности хранить такую драгоценность!.. Да лучше бы ты продал его! Да ты бы получил любые деньги, какие бы ни запросил, – на то и императоры, чтобы платить любую цену! А где теперь твой конь? Какое несчастье!”

Старик же сказал: “Ну-ну, не увлекайтесь! Скажите просто, что коня нет в стойле. Это – факт, все же остальное – суждения. Счастье, несчастье… Откуда вам это знать? Как вы можете судить?”

Люди сказали: “Не обманывай! Мы, конечно, не философы. Но и не настолько дураки, чтобы не видеть очевидного. Конь твой украден, что, конечно же, несчастье!” Старик ответил: “Вы – как хотите, а я буду придерживаться такого факта, что раз стойло пусто, то коня там нет. Другого же я ничего не знаю – счастье это или несчастье, потому что это всего лишь маленький эпизод. А кто знает, что будет потом?”

Люди смеялись. Они решили, что старик от несчастья просто рехнулся. Они всегда подозревали, что у него не все дома: другой бы давно продал коня и зажил как царь. А он и в старости оставался дровосеком: ходил в лес, рубил дрова, собирал хворост, продавал его и еле-еле сводил концы с концами, живя в бедности и нищете. Ну а теперь стало очевидным, что он – сумасшедший.

Но через пятнадцать дней конь неожиданно вернулся. Он не был украден, он сбежал в лес. И вернулся не один, но привел с собой дюжину диких лошадей. И снова собрались люди и сказали: “Да, старик, ты был прав! Это мы – глупцы! Да он и впрямь счастье! Прости нашу глупость милосердно!”

Старик ответил: “Да что вы, ей-богу! Ну вернулся конь. Ну лошадей привел – так что ж? Не судите! Счастье, несчастье – кто знает?! И это лишь маленький эпизод”…» и так далее… Таких маленьких эпизодов было очень много в жизни этого старика, как их много и у каждого из нас.

Поражение – это не всегда поражение. Оно только сейчас поражение, но благодаря ему приобретается мудрость, опыт и сноровка, которые становятся основой будущих побед. А обещанная мудрость – это разве поражение? Если мудрость – это плата за поражение, то что же тогда поражение? Теряется одно, приобретается совсем другое. Теряются материальные ценности, приобретается знание. Теряется время, приобретается поэтическое состояние души. Уходит забота, приходит радость.

В свете сказанного думается, что проблема безопасности, и информационной безопасности в частности, – вечная проблема, которая если и решается, то только на короткое мгновение, пока у субъекта соответствующее состояние души или, проще говоря, определенное состояние защищенности. Но из этого многопараметрического пространства, в котором единственным критерием, благословляющим на деятельность, является состояние субъекта, есть один правильный выход. Этот выход называется «сужение области исследования». Именно этим путем пошли авторы книги, назвав ее «Обеспечение информационной безопасности бизнеса». При таком подходе появляется способ измерить это самое мифическое состояние защищенности, которое теперь меряется совсем просто – скоростью изменения активов. В этой ситуации становится понятным, что такое ущерб и какими могут быть риски. Задача приобретает реальные очертания, и появляются вполне материальные критерии, которыми можно оперировать, используя классический инструментарий.

Вот только для случая информационной безопасности этот классический инструментарий уже несколько иной. А иной потому, что используется в других условиях. В условиях, когда человечество погрузилось в информационную эпоху и между человеком и человеком прочно встало техническое средство, способное генерировать, усиливать и блокировать любые информационные потоки. Более того, даже угрозы в этих условиях выглядят уже по-другому, их значимость смещается от угроз типа «украдут информацию» к угрозам «навяжут информацию». Потому что если информацию навяжут, то тем самым навяжут и внешнее скрытое управление.

Понятно, что состояние защищенности у человека, отдыхающего на пляже Сочи, и человека, защищенного броней танка, но который идет в атаку, разные. Хотя во втором случае сверху целый слой брони и поддержка огневой мощи.

Когда нет физических угроз, то и физическая защита не нужна, а вот информационная – нужна всегда. Поэтому совершенно правильно авторы акцентируют основное внимание на угрозах информационной безопасности. Ибо получение информации и на ее основе изменение знания – постоянный процесс. Если под знанием понимать совокупность сведений, выраженную в структуре системы и функциональных элементах этой структуры, то становится понятным, как определенные структурные модификации могут приводить систему чуть ли не к полному разрушению. И чем значимее информация для принятия решений, тем важнее грамотно построенная система обеспечения информационной безопасности, гарантирующая устойчивость развивающегося знания от угроз в информационной сфере.

Целью информационной угрозы является активизация действий, ответственных за нарушение привычного или запланированного режима функционирования, т. е. за вывод системы за пределы допустимого режима функционирования, либо отказ системы от определенных действий и / или ресурсов, необходимых для достижения собственных целей. Здесь и далее под допустимым режимом функционирования понимается такое функционирование информационной системы, которое обеспечено необходимыми материальными ресурсами для достижения поставленной цели. В информационную эпоху реализация угрозы в большинстве случаев осуществляется через искажение адекватности модели миру. Этой проблеме посвящено достаточно материалов данной книги, и это правильно. Система не всегда способна в реальном времени понять, является ли конкретное сообщение угрозой. Так, например, по сообщениям американской прессы, предупреждения о террористическом акте 11 сентября 2001 года были у спецслужб за несколько дней до трагедии, но им не придали нужного значения. Они не соответствовали той модели мира, которая именно в тот момент была доминирующей у аналитиков.

В свое время противник, окружив город и устраиваясь на ночлег, разжигал костры. В пределах видимости с крепостных стен у каждого костра располагалось по 5–7 воинов. А дальше, за пределами видимости, – по одному человеку у костра. Для «умных», умеющих считать и делать выводы, численность армии мгновенно увеличивалась в несколько раз. Получается, что всегда возможны ситуации, когда «умным» быть опасно, ибо во многом факт того, что сооб-

щения нарушают адекватность модели мира, зависит от самого информационного субъекта, от созданной им модели мира, от его образа мира.

Любое живое существо всегда имеет несколько каналов получения информации, которые частично подстраховывают друг друга. Точно так же любая сложная социальная система: фирма, государство, – также имеет несколько независимых каналов сбора информации об окружающем мире и о самой себе. Определенный параллелизм присутствует и при обработке информации аналитическими центрами. И только в том случае, если результаты и рекомендации совпадают, система «может считать», что ее модель мира адекватна миру. Однако в случае серьезного целенаправленного информационного «продавливания» тех или иных идей, событий, сообщений происходит деформация уровня восприятия, и порой на самом деле мало значимый элемент искажает картину мира. В результате этого искажения в социуме активизируются соответствующие действия (алгоритмы), необходимые для их обработки. Поэтому вопросам принятия решений и уделяется все больше внимания при решении задач по обеспечению информационной безопасности, тем более в бизнесе.

При этом авторы, исследуя данную проблему, специально акцентируют внимание на следующем важном нюансе: не всегда следование нормативным требованиям (в частности, ИСО серии 9000) повышает эффективность бизнеса и защиты этого самого бизнеса. Порой эти требования увеличивают объемы отчетных формализованных материалов, за которыми может и ничего не стоять.

Мне же хотелось добавить к сказанному еще и то опасение, что если конкурент знает, чем вы пользуетесь (каким инструментом), что делаете (какие процессы) и как делаете (в рамках каких регламентов), то для него проще организовать скрытое управление вами.

В целом данная работа с достаточной полнотой охватывает заявленные проблемы. Здесь читатель найдет и существующие модели менеджмента (управления), применимые для обеспечения информационной безопасности бизнеса, и модели непрерывного совершенствования, и стандартизированные модели менеджмента, а также модели COSO, COBIT, ITIL. Достаточно интересный материал по контролю и аудиту, а также по измерению и оцениванию информационной безопасности бизнеса.

С. П. Расторгуев,
профессор, доктор технических наук

Введение

В течение ряда лет мы наблюдаем, что в нашем обществе среди специалистов, так или иначе имеющих отношение к вопросам безопасности вообще и к вопросам информационной безопасности в частности, не снижается интерес к вопросам обеспечения информационной безопасности бизнеса.

Существует значительное число публикаций по различным аспектам безопасности (охрана, контроль доступа, физические аспекты безопасности, экономическая безопасность, информационная безопасность, охрана секретов, криптография, персональные данные, критические технологии, борьба с терроризмом, непрерывность бизнеса, катастрофоустойчивость, борьба с сетевыми атаками), каждое из которых в большей или меньшей степени претендует на некую точку зрения или интерпретации этого сложного вопроса применительно к бизнесу.

Следует также отметить, что общих подходов к проблеме, как правило, не формулируются, каждый рассматриваемый и анализируемый аспект отражает только профессиональные предпочтения специалистов.

В целом для ситуации характерен узкоспециализированный подход, взгляд на проблему сквозь призму профессиональных приверженностей, что никогда и нигде не способствовало пониманию вопроса и в конечном итоге – делу.

В этом многоголосии практическому специалисту, который реально занимается вопросами обеспечения безопасности собственной организации, достаточно сложно ориентироваться, найти ответы на возникающие вопросы, выработать правильный путь деятельности. Это подтверждают острота и накал дискуссий вспыхивающих практически по любому вопросу, как сейчас, например, по проблеме персональных данных.

Следует сказать, что наша страна в целом ориентируется на экономическую открытость, взаимодействие с западным бизнесом, нужна платформа для такого взаимодействия и в этом направлении сделаны настоящие революционные шаги – высшее руководство государства сформулировало задачу модернизации экономики. Один из практических шагов на этом пути – широкое использование зарубежных стандартов и лучших практик там, где до настоящего времени не удалось создать современных российских регламентов, стандартов и правил. С этой целью приняты соответствующие поправки в Федеральный закон «О техническом регулировании».

Остро встал вопрос трансграничного взаимодействия экономических субъектов, а также институтов государств. Для такого взаимодействия также нужны универсальные правила, понятные, приемлемые и одинаково применимые в странах, где находятся субъекты этих отношений.

На этом фоне безопасность, как специфическая отрасль знаний и еще более специфическая научная дисциплина, переживает исключительно динамичный этап развития.

Коротко напомним этапы ее развития.

На протяжении тысяч лет под обеспечением безопасности информации понималась исключительно задача обеспечения ее конфиденциальности. Были испробованы разные способы обеспечения конфиденциальности – от тайнописи и использования незнакомого иностранного языка для скрытия информации от недруга до отрезания языка носителю информации, что было, видимо, эффективно в условиях, когда письменностью владели единицы людей и онемевший носитель не мог передать никому свое знание секрета. В итоге конкуренции методов обеспечения конфиденциальности развилось и победило новое научное направление – криптография, в котором работали и работают выдающиеся математики как прошлого, так и современности. Это направление получило два толчка в XX веке – радио представило новую возможность передачи информации по «эфиру», и сразу возникла необходимость пере-

давать по открытым «эфирным» каналам большие объемы конфиденциальной информации, а несколько позже появились вычислительные машины, сначала аналоговые, несколько позже электронные, которые сразу были использованы для решения двух задач: создание эффективных шифров и алгоритмов и их «взлом».

Широкое применение во время Второй мировой войны авиацией и флотом фашистской Германии шифровального оборудования – роторных шифровальных машин «Энигма», с одной стороны, и необходимость повышения эффективности боевых действий союзников на суше и операций по борьбе с фашистскими подводными лодками, представлявшими крайне серьезную угрозу, – с другой, породили новые направления в радиоразведке и технической защите информации.

Это была борьба за повышение качественных показателей систем дешифрования, пеленгации и радиоразведки, в том числе и путем использования слабостей (уязвимостей) технического оборудования, как, например, попыток пеленгации германских лодок по излучениям гетеродинов их приемников, а с другой – борьба с побочными излучениями радиоприемников, позднее ЭВМ, паразитными высокочастотными генерациями усилителей, и наводками в цепи питания шифровальных машин. Первые опыты по исследованию побочных электромагнитных излучений электронного оборудования ставились еще в фашистской Германии во время войны. Таким образом, техническая защита информации как классическая техническая отрасль деятельности в составе перечисленных направлений сформировалась около 70 лет назад. Возраст солидный. При этом следует отметить, что в этой парадигме доминирует инженерный, «радиотехнический», строго детерминированный подход. В этой системе взглядов таких понятий, как «риск», «право субъекта на выбор приемлемых защитных мер под возникающую ответственность», «проактивные меры защиты», просто не существовало и не могло существовать.

Следующий толчок в развитии проблемы дало широкое внедрение в практическую жизнь средств вычислительной техники в 1960–1970-е гг. В это время сервисы информатизации, которые ранее были уделом узкого круга специалистов, стали доступны широким слоям обычных людей, в основном работникам фирм и организаций. От основного, военного направления в криптографии возникла боковая ветвь – гражданская криптография, направленная кроме основных традиционных целей на обеспечение целостности несекретной информации.

И наконец, в 1980-е гг. все существенно изменилось в связи с появлением персональных ЭВМ и чуть позже – возникновением сети Интернет.

В середине 1970-х гг. в связи с созданием крупных баз данных и переводом все больших объемов информационных ресурсов в цифровую форму в проблеме защиты информации наметился сдвиг от инженерного подхода к вопросам информатики в область управления доступом к вычислительным и информационным ресурсам, что нашло отражение в итоге в создании в США знаменитой «оранжевой книги», использованной впоследствии для разработки отечественных требований по защите информации в автоматизированных системах Гостехкомиссии СССР (позднее ГТК России, сейчас ФСТЭК).

Но потенциал этой идеи в силу ее статичности был достаточно быстро исчерпан, в середин 1990-х гг. «оранжевая книга» как отжившая идея была публично сожжена, а международными экспертами в области безопасности в примерно в одно время было сформировано два направления развития – создание технических стандартов по обеспечению безопасности продуктов информационных технологий под общим названием «Общие критерии» и создание семейства стандартов качества, а в последнее время – управления, под обобщенным названием «Стандарты аудита безопасности».

Стало очевидно, что «Общие критерии» не получили широкого распространения в силу ряда причин (ограниченность сферы применения, сложность и ограниченность используемых механизмов оценок), поэтому началась их активная доработка в направлении второй группы

стандартов, а сама группа стандартов аудита обогатилась концепцией «риск-ориентированного подхода», что означало фундаментальные изменения в концептуальных взглядах на проблему безопасности в целом и сдвиг проблемы защиты информации, а если точнее – информационной безопасности в сферу управления сложными техническими системами и коллективами, как эксплуатационного персонала, так и пользователей.

В последнее время в теории и практике управления возникло еще одно направление – создание стандартов управления организациями, имеющее своей целью оптимизацию внутренней структуры организации для получения максимального результата от их деятельности (реинжиниринг). Появились «Стандарты управления деятельностью организаций», которые рассматривают общие вопросы управления сложно организованными коллективами людей.

Но если говорить о безопасности как научной дисциплине, то, пожалуй, впервые за все время она подверглась анализу и глубоким разносторонним исследованиям, что, по-видимому, и послужило толчком для последних разработок на базе риск-ориентированных подходов.

Целесообразно напомнить основные выводы этих исследований.

Объект защиты, т. е. то, к чему прикладываются сервисы безопасности с целью придать этому объекту важное дополнительное, изначально отсутствующее свойство – защищенность (надежность, устойчивость), представляет собой в абсолютном числе случаев сложную систему. При этом в практической жизни мы, как правило, имеем дело со сложными системами, составленными в свою очередь не из простых элементов, а сложных систем. Таким образом, мы имеем дело со «сложными системами сложных систем».

Применительно к вопросам безопасности следует учитывать следующие свойства сложных систем:

– наиболее вероятный отклик сложной системы на единичное воздействие – хаотический;

– сложная система обладает новыми иными свойствами, нежели совокупность свойств элементов, составляющих эту систему;

– отклик сложной системы на воздействие является нелинейным и изменяется в зависимости от силы этого воздействия. Новые свойства системы при слабых воздействиях могут не проявляться, поэтому нельзя с уверенностью сказать, что свойства конкретной сложной системы полностью изучены и ее поведение под воздействием мощного воздействия предсказуемо.

Безопасность как самостоятельный объект исследования также имеет некоторые фундаментальные свойства:

– безопасность никогда не бывает абсолютной – всегда есть некий риск ее нарушения, таким образом, усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого уровня, не более;

– измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности системы; в связи с этим можно говорить только о вероятности наступления того или иного события и степени его последствий, т. е. использовать для оценок уровня безопасности рисковый подход;

– наступление рискового события в общем случае предотвратить невозможно, можно лишь понизить вероятность его наступления, т. е. добиться того, что такие события будут наступать реже;

– можно также понизить степень ущерба от наступления такого события, но при этом чем реже наступает рисковое событие, тем сильнее ущерб от них;

– при любом вмешательстве в систему в первую очередь страдает ее безопасность.

Оказалось, что для анализа свойств безопасности сложных систем, состоящих из технических компонент людей, взаимодействующих друг с другом, в полной мере могут быть применены некоторые социологические и психологические правила, выведенные на основе наблюдения за развитием процессов и событий:

• Закон Парето (универсальный закон неравенства), сформулированный итальянским экономистом и социологом Вильфредо Парето в 1897 г., более известный как шутливое выражение «20% немцев выпивает 80% пива», в соответствии с которым первые 20% усилий дают 80% результатов или 80% всех проблем порождаются человеком (персоналом) и лишь 20% приходится на долю технического оборудования (по оценкам специалистов, эта доля может доходить до соотношения 94:6%).

• Методологический принцип, получивший название по имени английского монаха-францисканца, философа-номиналиста Уильяма Оккама (Ockham, ок. 1285–1349), гласящий: «То, что можно объяснить посредством меньшего, не следует выражать посредством большего» (лат. Frustra fit per plura quod potest fieri per pauciora). В соответствии с ним при равной вероятности событий с различной степенью тяжести последствий, как правило, первым случается событие, степень тяжести последствий которого меньше. Из этого также следует, что злоумышленник, планируя атаку на ресурс, из всех возможных будет выбирать наиболее простой способ осуществления своих целей, а вирусы будут попадать в систему наиболее простым способом. Этот принцип следует дополнить следующим наблюдением: степень тяжести последствий растет обратно пропорционально частоте их возникновения.

• Правило связиста: связиста замечают только тогда, когда пропадает связь.

• Парадокс «крысиного короля», хорошо знакомый морякам: можно избавиться от крыс на корабле, заведя крысу – «крысоеда», но через некоторое время он даст потомство, бороться с которым будет еще сложнее. Таким образом, налицо эффект транспонирования проблемы в будущее, через точку инверсии.

Как уже отмечалось, аспектов обеспечения информационной безопасности бизнеса достаточно много, но в целом есть и ряд общих моментов, на которых следует коротко остановиться.

Ведение бизнеса всегда предполагает наличие некого первоначального капитала, актива, который вкладывается в некое «дело» с целью получения прибыли. Все остальное, не имеющее актива, к бизнесу не относится и не рассматривается.

Эффективность бизнеса тем выше, чем выше прибыль – это аксиома. На величину прибыли влияет несколько факторов, среди них выделяются наиболее существенные:

– величина внутренних издержек, в том числе на содержание коллектива и затрат на обеспечение безопасности в том числе. В результате задания неправильных требований по безопасности, величина издержек может стать настолько обременительной, что сделает бизнес не эффективным;

– качество управления собственным активом. Если кроме собственника актива или его представителя активом может управлять еще кто-то в собственных интересах, то актив может разворовываться, а бизнес – существенно ухудшаться. Пример перед глазами – хищение средств в карточных платежных системах и в системах дистанционного банковского обслуживания;

– качество работы коллектива, обеспечивающего бизнес;

– скорость реакции коллектива на внешние факторы, влияющие на бизнес, или на управляющие воздействия;

– стратегия и качество ведения самого бизнеса;

– выбранная стратегия управления рисками, в том числе экономическими рисками и рисками информационной безопасности.

Следует также отметить, что бизнес ведется, как правило, во враждебной среде, в условиях конкурентной борьбы, неблагоприятного законодательства, риска рейдерства, часто нескоординированной деятельности различных надзорных органов. Особое место в этом списке занимает криминал, стремящийся отнять или поставить под контроль прибыль от вложения активов. Наиболее в острой форме это появляется в банковском бизнесе, поскольку банки работают с самой сублимированной формой активов – деньгами, а атака на них наиболее результативна, потому что приносит быстрые и ощутимые результаты.

Поэтому все большее значение приобретает прогноз, то есть моделирование возможных рисковых ситуаций и разработка превентивных защитных мер, позволяющих избежать (отразить, уклониться) последствий от атак на бизнес или на среду, обеспечивающую использование активов, составляющих основной элемент бизнеса.

Также следует отметить, что среди всего набора угроз и рисков существует определенная иерархия, по силе воздействия и уровню катастрофичности для бизнеса угрозы серьезно различаются. Так, политические риски или риски несоответствия законодательству являются для бизнеса определяющими, так как способны вне зависимости, насколько качественно осуществляется работа по минимизации рисков информационной безопасности физически уничтожить бизнес (лишение лицензии, налоговые штрафы и т. д.). К сожалению, следует говорить и о рисках, возникавших и при взаимодействии с правоохранительными органами, например, когда в ходе расследования изымались оригиналы документов или сервера с базами данных, что неминуемо ведет к катастрофическим последствиям для организации.

С другой стороны, при абсолютно благоприятном внешнем политическом, законодательном и экономическом фоне, реализация рисков информационной безопасности может нанести субъекту бизнеса ущерб такого размера, от которого оправиться крайне сложно.

Таким образом, существует ряд рисков, включая риски информационной безопасности, ущерб от которых может быть неприемлем для субъекта бизнеса. В то же время некоторые общие риски политического, экономического и правового характера обладают «кумулятивным» эффектом и способны нанести системный ущерб, затрагивающий практически все сферы деятельности организации.

Что касается угроз информационной безопасности бизнеса, то их условно тоже можно разделить на две группы:

– традиционные угрозы безопасности информации, такие как нарушение конфиденциальности или неправомерное использование информации, реализуемые через новые механизмы, возникшие в результате использования информационных систем;

– новые угрозы, порожденные спецификой информационных систем – вирусы, сетевые атаки, нарушения функционирования и отказы разного рода, всевозможные нарушения персоналом установленных регламентов, инструкций и предписаний по эксплуатации и обслуживанию информационных систем.

Эти и другие вопросы авторы постарались рассмотреть в книге, предлагаемой вниманию читателя.

1
Философия информационной безопасности бизнеса

1.1. Бизнес и информация

1.1.1. Информационная сущность бизнеса

Информация является неотъемлемой частью бизнеса. Бизнес-процессы не могут существовать без информации и вне информации, хотя бы потому, что бизнес существует в рамках определенной правовой среды, определяемой совокупностью информационных объектов, таких как законодательные и нормативные акты, постановления правительства и другие подобные документы, и формирует отчетность по нормам этой правовой среды, т. е. порождает информацию определенного вида. Сущность бизнес-процесса представляется как процесс достижения некоторой совокупности целей (бизнес-целей) на основе *управления* активами. Информационной сущностью бизнеса и является этот процесс управления. Если правовое поле, отчетность, активы и возможные операции над ними во многом зависят от природы бизнеса, то процесс управления в большой степени инвариантен к ней.

Главная особенность управления в бизнесе, существенно отличающая его от некоторых других, например технических систем автоматического управления и регулирования, является большая задержка между моментом принятия решения и получаемым результатом, что иллюстрирует рис. 1. После принятия решений по управлению реализуется некий процесс бизнеса, протекающий в слабодетерминированной внешней среде, не все параметры которой контролируются организацией, осуществляющей бизнес. Таким образом, результат принятых решений наблюдается с задержкой и иногда весьма значительной. Поэтому важнейшей для бизнеса является способность предвидеть возникновение разного рода ситуаций (как благоприятных, так и неблагоприятных) в среде бизнеса и в самом бизнесе. Это чисто информационная задача, в основе которой лежит прогноз.

Рис. 1. Особенность управления в бизнесе

Когда задумывается и реализуется какой-либо процесс целенаправленной деятельности необходимо поставить и ответить на следующие вопросы.

• Будет ли достигнута цель в том виде, как предполагается?

• Достаточно ли в нашем распоряжении операционных возможностей, знаний (опыта), соответствует ли потребностям качество подготовки персонала и система менеджмента?

• Достаточно ли привлечено ресурсов для достижения поставленной цели?

• Достаточен ли интервал времени, устанавливаемый для достижения цели?

Из поставленных вопросов видно, что ответы на них требуют анализа различных информационных сущностей, описывающих в формализованном или неформализованном виде различные аспекты деятельности, отраженные в заданных вопросах. Ясно, что ответы на эти вопросы могут быть получены только в виде прогнозов, т. е. тоже в виде информационных сущностей. Очевидно также, что все вопросы взаимозависимы и, следовательно, ответы на них должны быть взаимоувязаны. Совокупная погрешность ответов на вопросы создает консолидированный риск достижения цели. Величина этого риска зависит еще и от того, насколько изменятся условия реализации цели в процессе ее достижения, и от характера этих изменений.

1.1.2. Информационные характеристики бизнеса

Необходимые для прогноза данные: все прошлое и будущее, включая любые формулировки целей и планы их реализации, вся среда бизнеса и вообще материальный мир – существуют в виде описаний, т. е. в виде информации. Чем больше интервал времени T и связанный с ним прогноз (см. рис. 1), тем лучше должен быть организован бизнес. Но тем труднее сделать точный прогноз, и тем более качественная информация для него требуется. Информационное поле бизнеса или его информационная сфера образуется из:

– правовой среды (законодательных и нормативных актов, постановлений правительства и прочих документов);
– отчетности по нормам правовой среды;
– специфичной информации бизнеса.
Эта последняя информация наиболее динамична и включает:
– субъекты, объекты и процессы бизнеса, представленные в информационном виде;
– нормативную, организационно-распорядительную и иную документационную базу организации;
– данные мониторинга бизнес-среды и собственной среды;
– аналитические данные (обзоры) и прогнозы состояния внешних и внутренних факторов влияния;
– накопленные и обобщенные практики (знания);
– стратегические и оперативные планы организации и решения по ним.

Качество информации, используемой для прогноза при принятии решений, определяется не только количеством используемых данных, но и (в наибольшей степени) тем, как эти данные систематизированы и обобщены, насколько адекватно используемые понятия, теоретические построения и представления отражают материальный мир и среду бизнеса и организации. Поэтому надо говорить не просто о данных или информации, а о знаниях, помогающих рационально организовывать деятельность организации по достижению поставленных целей и решать различные проблемы, возникающие в процессе этой деятельности. Следовательно, главная проблема бизнеса в информационной сфере – проблема накопления хорошего знания, являющегося единственной гарантией точности прогноза.

Основные требования к качеству информации и знаний иллюстрирует рис. 2. Данные нижнего уровня пирамиды управления, накапливаясь и подвергаясь систематизации и обобщению, должны превращаться в отфильтрованную полезную информацию, а затем накапливаться в виде знаний и использоваться на всех уровнях иерархии управления.

С точки зрения возможностей по накоплению знаний можно выделить информационно опасные виды бизнеса. Признаки, позволяющие отнести бизнес к информационно опасному виду:

– бизнес, требующий долговременных инвестиций: здесь требуется очень долговременный прогноз, который сделать практически невозможно, ситуация усугубляется, если инвестиции делаются в новое, слабо исследованное направление;

– бизнес, реализующийся в сильно изменчивой среде: основная сложность организации такого бизнеса состоит в накоплении знаний, как следствие точный прогноз становится невозможен;

– краткосрочный (однократный) бизнес, требующий быстрого накопления знаний: организаторы бизнеса, как правило, надеются на «удачу» и часто проигрывают;

– абсолютно новый вид бизнеса: накопление знаний происходит в процессе развертывания бизнеса, осуществляемого путем инвестиций мелкими порциями, при этом часто оказывается необходимой модификация первоначально поставленной цели;

– бизнес «реального » времени – условия (среда) изменяются одновременно с возвратом инвестиций: знания невозможно накопить вообще.

В настоящее время наблюдается существенное повышение роли информатики в бизнесе, что обусловлено информационными характеристиками современного бизнеса. Информационная составляющая бизнеса постоянно растет, и рост ускоряется. Прежде всего это резкий рост факторов, влияющих на успешность бизнеса, и их пространственно-временная распределенность. Стремление организаций учесть максимальное число таких факторов в условиях сокращения времени на принятие решений, приводящего к необходимости быстрой обработки большого количества информации, требует использования соответствующих технических средств, компьютерных сетей и телекоммуникаций. Эти потребности и стремление к снижению издержек все больше перемещают бизнес из материального мира в информационный. Но одновременно при сокращении времени на принятие решений затрудняется проверка достоверности информации, на которой эти решения должны быть основаны. Необходимость повышения точности прогноза и принимаемых решений сопровождается неполнотой, неточностью и несвоевременностью получаемых и используемых для него данных.

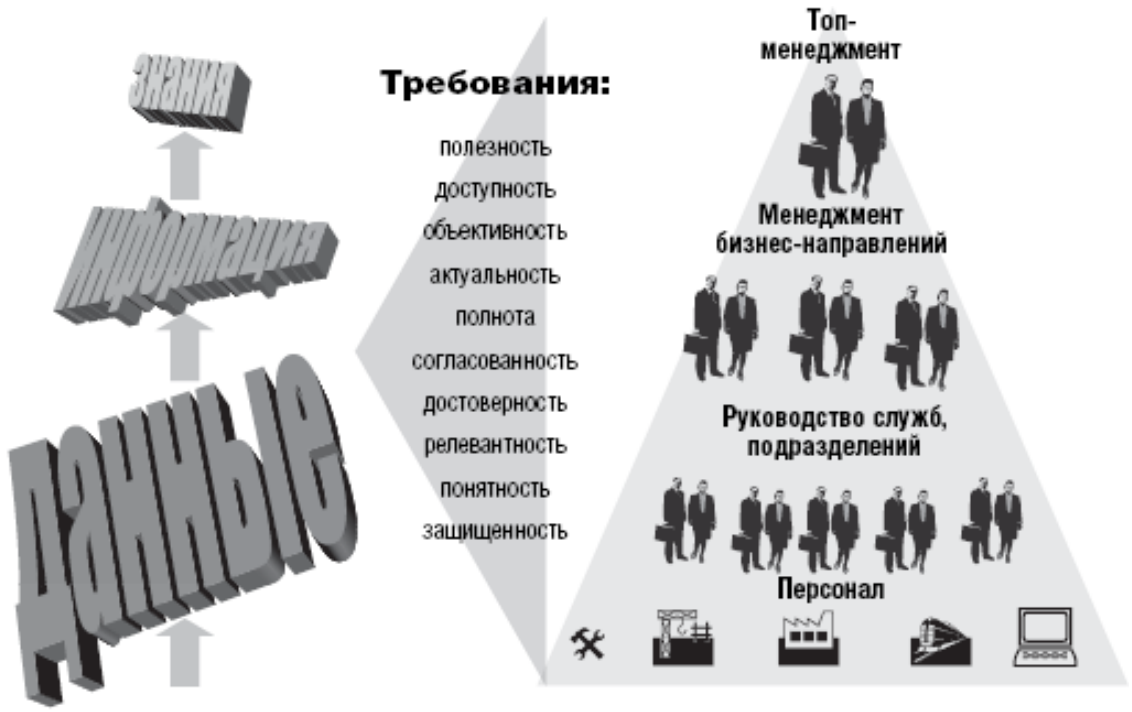

Рис. 2. Качество информации определяет качество и эффективность управления

1.1.3. Уязвимости процессов накопления знаний (самообучения)

Сам по себе процесс получения и накопления информационного знания, или процесс самообучения, внутреннее свойство любого бизнеса. Проблема в том, что этот процесс уязвим. Его уязвимость во многом определяется свойствами и особенностями информационной сферы, подробно рассмотренными в следующем разделе. Отчасти эти особенности проистекают из свойств информации как таковой: невозможность создания точного информационного образа материального мира, неизменность информационных объектов во времени, приводящая к возникающей неадекватности описаний реальным (стареющим) объектам, противоречивость и неполнота нормативно-правовой базы и т. п. Чрезвычайно существенный фактор – низкая информационная культура использования информационной сферы. Чтобы обеспечить необходимые свойства и качество информации, надо прикладывать соответствующие усилия. Если информационную сферу бизнеса или организации специально не организовывать, придавая ей определенную структуру и наделяя необходимыми полезными свойствами, то она превращается в шум. В ней возникают разрывы, всякие коллизии, она заполняется мусором, неактуальными сведениями, что и означает «низкая информационная культура». Неадекватные, неправильные и бесполезные знания не позволят делать точные прогнозы, принимать правильные решения, и бизнес придет в упадок. Таким образом, «стихийное» самообучение и накопление знаний необходимо соответствующим образом направлять и организовывать, реализуя в информационной сфере комплекс мер, способствующий тому, чтобы она была адекватная, качественная и обладала свойствами, полезными для бизнеса и организации.

Другие уязвимости процесса самообучения вызваны особенностями осуществления любого бизнеса и тем конфликтом интересов, который проистекает из этих особенностей. Рассмотрим подробнее, причем будем идти не от уязвимостей, а от того, каким образом бизнес или организация могут получить преимущества для себя, поскольку это основная цель бизнеса и организации при накоплении и обобщении знаний. Решающее значение для получения преимуществ в бизнесе имеет точный прогноз, осуществляемый на основе этих знаний.

Менеджмент организации обычно требует как можно более точного и продолжительного прогноза. Возникает вопрос: насколько точным и долговременным должен быть прогноз реально? Эти характеристики зависят от вида и природы бизнеса и величины участвующих в деле активов (см. признаки информационно опасного бизнеса). Но на практике, чтобы получить преимущество, достаточно иметь лучший и более продолжительный прогноз, чем у других участников бизнеса. Чтобы получить преимущество, есть три способа, обычно используемых в сочетании друг с другом.

Во-первых, необходимо обеспечить более эффективное обучение и накопление знаний. Условиями быстрой сходимости и эффективность процесса накопления знаний (обучения) является полный доступ к:

– исходной информации, используемой для накопления знаний, всех субъектов, участвующих в бизнесе организации;
– уже накопленным знаниям, опыту и частично обработанной информации.

Во-вторых, преимущество можно получить, мешая другим организациям (как конкурентам, так и союзникам) и субъектам получать нужные знания путем соответствующих информационных воздействий. Здесь в основном два пути.

Навязать заведомо ложную либо существенно неполную, искаженную, но во всех случаях правдоподобную информацию. Чем ее больше, тем лучше, поскольку в этом случае облегчается прогноз поведения противоборствующей стороны. Неправильные прогноз и целеполагание, выполненные противоборствующей стороной и основанные на известной нам (навязанной) ложной информации, снимут часть неопределенностей в прогнозе для своего бизнеса и организации.

Скрыть свой опыт. Накопление знаний противоборствующей стороной требует информации, и чем больше ее получат противоборствующие субъекты, тем лучше они смогут построить свой прогноз. Отсюда следует необходимость минимизировать выходящую за пределы организации информацию, и в первую очередь должна быть минимизирована информация о целях.

Это не что иное, как один из элементов информационного противоборства. Основная его опасность в том, что он наиболее эффективно действует именно на систему управления – основную сущность бизнеса. Это та область, где информационная атака может существовать самостоятельно, а не как вспомогательное средство для атак в других базисах (экономических, финансовых, юридических и т. п.).

Отметим, что классическое информационное противоборство не предполагает наличия каких-либо правил, ограничивающих действия сторон. Однако бизнес-сообщество должно иметь (и, как правило, имеет) свои «правила игры», определяющие некоторую этику поведения, т. е. что можно, а что нельзя. Основой таких правил может служить, например, общая корпоративная цель у кредитных организаций, в отрасли и т. п. Другой пример – введение ограничений на возможность разрушения чужих целей. Маскирующая информация только должна скрывать свои цели (подобно ограничениям на рекламу товаров). Законодательная база в нашей стране слабо регулирует эту область.

В-третьих, получить преимущество можно, используя чужие (украденные) знания. Теоретически чужие знания могли бы быть полезны в двух аспектах:

– для прогноза состояния противоборствующего субъекта;
– для использования в своей деятельности.

Располагая общедоступной информацией и зная методы, методики, алгоритмы ее использования и обработки можно с достаточной точностью предсказать будущее поведение субъекта

бизнеса (организации). Этот аспект использования чужих знаний не вызывает особых сомнений, и полезность получения информации о чужом опыте неоспорима.

Что касается использования чужих знаний в своей деятельности, то этот вопрос весьма спорен. Многочисленные примеры, в том числе исторические, свидетельствуют, что воспользоваться чужими знаниями в своей деятельности не удается. Это обусловлено тем, что знания – сильно структурированная информация, которая может правильно интерпретироваться и эффективно использоваться только соответствующей инфраструктурой (включая «мозги» субъектов, работающих в организации). Чтобы воспользоваться чужими знаниями надо «украсть» (или купить) всю инфраструктуру. Если вместо этого создавать свою (под чужие знания), то будет упущено время, противодействующая сторона уйдет вперед и получит преимущество в бизнесе.

Теперь остается поставить себя на место конкурента, который также желает получить для себя преимущества, и получим основные уязвимости процесса самообучения.

Во-первых, полный доступ к информации, знаниям и опыту организации, обеспечивающий эффективное самообучение, сам по себе является одновременно уязвимостью. Реально во всех организациях внутренняя информация, хотя бы неформально, категорируется по степени важности и ограничениям в доступе и доступ к чувствительной информации как-то регулируется. Вторая уязвимость, связанная с эффективностью, – уже обсуждавшаяся общая информационная культура работы с информационной сферой организации. Чтобы персонал организации мог своевременно получить доступ к нужной ему адекватной и точной информации, она должна быть соответствующим образом организована.

Во-вторых, перед принятием решений по крупным бизнес-проектам велик риск создания и навязывания конкурентами потоков ложной и маскирующей информации, возможно, по нескольким независимым каналам. Эта угроза усугубляется специально созданным (конкурентами же) дефицитом времени или другими условиями (например, атакой на доступность серверов с базами данных), не позволяющими проверить достоверность этой информации или затрудняющими эту проверку. Отметим, что активность конкурентов, скорее всего, нельзя будет назвать злоумышленной, они просто пытаются взять свое, реализовать свой бизнес, о существовании вашей организации и ее участии в бизнесе они даже могут и не знать.

В-третьих, всегда есть риск, что данные, принадлежащие организации, будут похищены или она будет поставлена в условия, когда будет вынуждена хотя бы частично их предоставить, например, участвуя в конкурсах и тендерах на выполнение проектов. Защититься от использования ваших знаний конкурентами в своей деятельности, включая противодействие утечке через переманивание персонала, можно за счет децентрализации знаний. Защититься от использования вашей информации в других целях значительно сложнее. Как правило, это инсайдерская информация. Наиболее опасны менеджеры высшего уровня, владеющие большим объемом особо ценной информации. В любом случае угроза хищения данных тем больше, чем более доступна чувствительная для организации информация. Таким образом, есть противоречие с эффективностью накопления знаний, где важно, чтобы знания были всем одинаково доступны.

Низкий ресурсный порог информационных воздействий, а также то, что информация ничего не стоит до момента ее использования, существенно понижают психологический порог субъектов и усиливают их склонность к нарушениям (несоблюдению правил) в информационном мире. Это усугубляет ситуацию и увеличивает риск реализации угроз хищения и информационного противоборства.

1.1.4. Определение информационной безопасности

Постепенное осознание факта, что информационное воздействие на бизнес-процесс (на управление им) может быть эффективнее, чем материальное или финансовое воздействие, а также низкий ресурсный порог таких воздействий превращают информационное противоборство в главный инструмент выживания и конкурентной борьбы. А это, в свою очередь, выводит на первый план роль информационной безопасности, которая должна быть неразрывна с бизнесом.

Под *информационной безопасностью* (ИБ) организации понимается состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере.

Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений. Рассмотрим основные свойства информационной сферы, важные с точки зрения ИБ.

1.2. Материальные и нематериальные (информационные) аспекты бизнеса

1.2.1. Общая структура информационной сферы. Связь с материальным миром

Реальное управление активами организации в процессе реализации любого бизнеса осуществляется менеджментом на информационном уровне. Любые операции с материальными активами, как правило, сопровождаются параллельно выполняемыми операциями с их информационными описаниями или представлениями. Например, для основных средств организации при их приобретении такими представлениями являются товарные накладные, внутренние документы на оприходование, карточки учета основных средств, договоры на выполнение пусконаладочных работ, акты ввода в эксплуатацию основных средств и т. д.

Операции с материальными активами сопровождаются, как правило, финансовыми операциями, которые также отображаются на информационную сферу. Для нашего примера это оплата стоимости основного средства его продавцу или производителю по выставленным счетам, счета-фактуры, сопровождающие поставку изделия, с информацией для учета налога на добавленную стоимость, расчеты по договорам выполнения пусконаладочных работ и т. п. Эти операции выполняются с участием банковской системы, где также остаются информационные следы операций в виде информации о выполненных проводках.

Если материальные объекты всегда имеют в среде организации свой информационный образ, то у некоторых информационных объектов в материальном мире эквивалента нет. Это отношения между субъектами и отношения между субъектами и объектами материального мира. Например, таковым является право субъекта на объект – некоторая информационная сущность (правоустанавливающий документ), которая всеми признается. Предъявив эту информационную сущность, субъект может заполучить себе материальный объект.

Параллельное существование, движение и взаимодействие объектов в реальном (материальном) и информационном мире иллюстрируется моделью на рис. 3. Часть транзакций с объектами может происходить в материальном виде, а часть – в информационном. Частично это управление, а частично – транзакции с описаниями материальных объектов. При этом действия над материальными объектами сопровождаются, а в некоторых случаях заменяются, действиями над их описаниями. Например, одной из процедур может быть предъявление права на материальный актив в виде информационного объекта (правоустанавливающего документа), описывающего отношения владения между информационными представлениями объекта и субъекта. Материальный объект в этом случае никак не участвует в операции, он не подвергается никаким изменениям, может не перемещаться в пространстве, более того, может вообще не существовать в материальном мире, для выполнения операции достаточно иметь только его информационный образ.

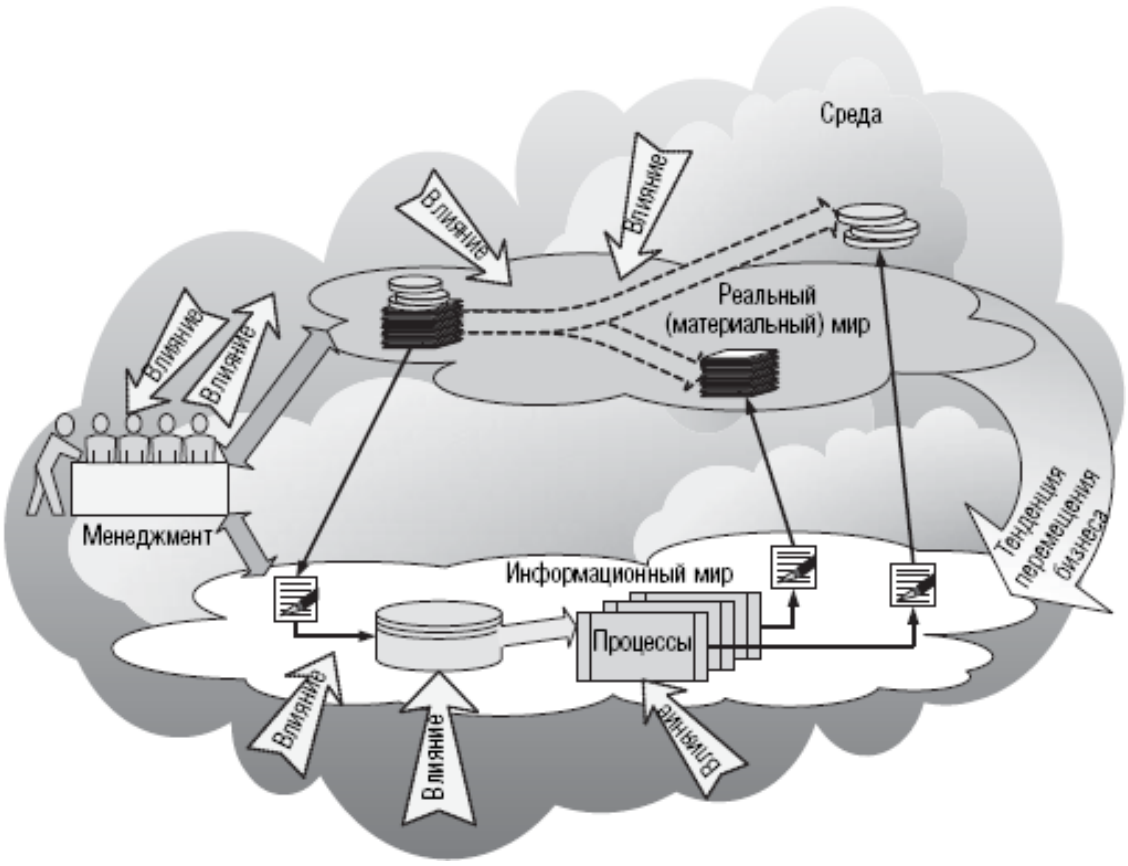

Рис. 3. Взаимодействие материального и информационного миров

Понятно, что целенаправленная деятельность будет нормально осуществляться в том случае, если реальный мир и информационный мир адекватны друг другу. Однако полного их соответствия друг другу нельзя достичь даже теоретически, так как в реальном мире объект зависим от времени, он «стареет», подвергается изменениям, в то время как его описание, полученное в какой-то момент времени, остается далее неизменным. В этой связи могут возникать либо искусственно создаваться различного рода коллизии. Например, реально объект существует, а его информационные следы отсутствуют. В этом случае он может быть «безболезненно» нештатно изъят из системы «реальный информационный мир» и использован в других целях. Наоборот, наличие «избыточного» информационного образа приведет в конце концов к возможности или необходимости штатного изъятия реального объекта, которого на самом деле нет, что в свою очередь создаст дефицит ресурса, не позволит достичь поставленной цели.

Риск возникновения подобных коллизий есть свойство информационной сферы. Главный источник этого риска – сам бизнес, особенно если он большой и территориально распределенный. Наиболее вероятная угроза, связанная с реализацией рисковых событий, приводящих к коллизиям, – конфликт интересов внутри организации. Персонал организации и особенно субъекты ответственности, менеджеры верхнего и среднего уровней, имея цели, отличные от целей организации, могут использовать ее активы (информацию, материальные активы, ресурсы) в своих интересах.

Конкретная реализация таких угроз потребует, чтобы бизнес стал слабо детерминированным, что затруднило бы его проверку. Стохастическая составляющая бизнеса не может быть проверена, и очень плохо, если она большая в силу самой природы бизнеса. Наиболее легко придать бизнесу стохастический характер именно в информационной сфере, замаскировав информационные воздействия под естественную случайность. Целью информационных

воздействий является в первую очередь ослабление контроля за счет создания иллюзии, что бизнес-процесс идет нормально и эффективно. Наиболее характерные примеры: искажение отчетности и лоббирование при принятии решений. В обоих случаях результатом, как правило, являются необоснованное увеличение (раздувание) активов и выделение («выколачивание») для «своего» подразделения организации избыточного ресурса. Избыточные активы и ресурс затем используются в своих интересах. Это всем известная схема превращения информации в материальную выгоду. Ущерб от конфликта интересов может значительно превосходить потери от злоумышленных действий, и, что страшнее, конфликт интересов реально приводит к потере управления.

Тенденции современного мира таковы, что бизнес, стремясь уменьшить издержки за счет ускорения процессов, все больше уходит в информационный мир, действия над материальными объектами во все большей степени замещаются действиями над их описаниями, т. е. над информацией. Эта тенденция и есть главный источник проблем информационной безопасности, поскольку в результате не только становятся возможными атаки с очень низким ресурсным и психологическим порогом их осуществления, но даже при отсутствии злоумышленных действий просто негативные свойства самой информационной сферы начинают отрицательно воздействовать на бизнес и приводить к серьезным потерям.

Говоря о свойствах информационной сферы, необходимо детализировать состав информационных объектов, входящих в нее. Для этого рассмотрим фрагмент структуры информационной сферы организации, показанный на рис. 4, где приведены наиболее характерные для современных организаций составные части:

– правовая среда бизнеса, находящаяся, как правило, за рамками конечных пользователей, предприятий и организаций;

– учредительная и лицензионная база организации (предприятия);

– специфичная информация бизнеса, которая, в свою очередь, может быть классифицирована на несколько видов, наиболее важные из них показаны в нижней части рис. 4.

Информационной основой деятельности менеджмента (см. рис. 4) является внутренняя отчетность организации и накопленные знания – аналитика и модели, систематизирующие и обобщающие информацию, необходимую для прогноза и принятия решения. Основная задача внутренней отчетности – предоставить руководству и менеджменту сжатую и своевременную информацию для быстрого и успешного принятия решений. Одновременно решается задача контроля в организации, начиная с контроля того, достигаются ли высокоуровневые, стратегические цели (бизнес-цели), и заканчивая контролем выполнения оперативно-тактических задач и контролем качества производимых продуктов.

Входные информационные потоки (информация о состоянии, предполагаемые последствия деятельности в виде прогнозов) превращаются менеджментом в управляющую информацию: оперативную – планы, распоряжения; стратегическую – цели, концепции, политики. Отношения субъект / субъект и субъект / объект, включая управление, обозначены на рисунке 4 синими линиями.

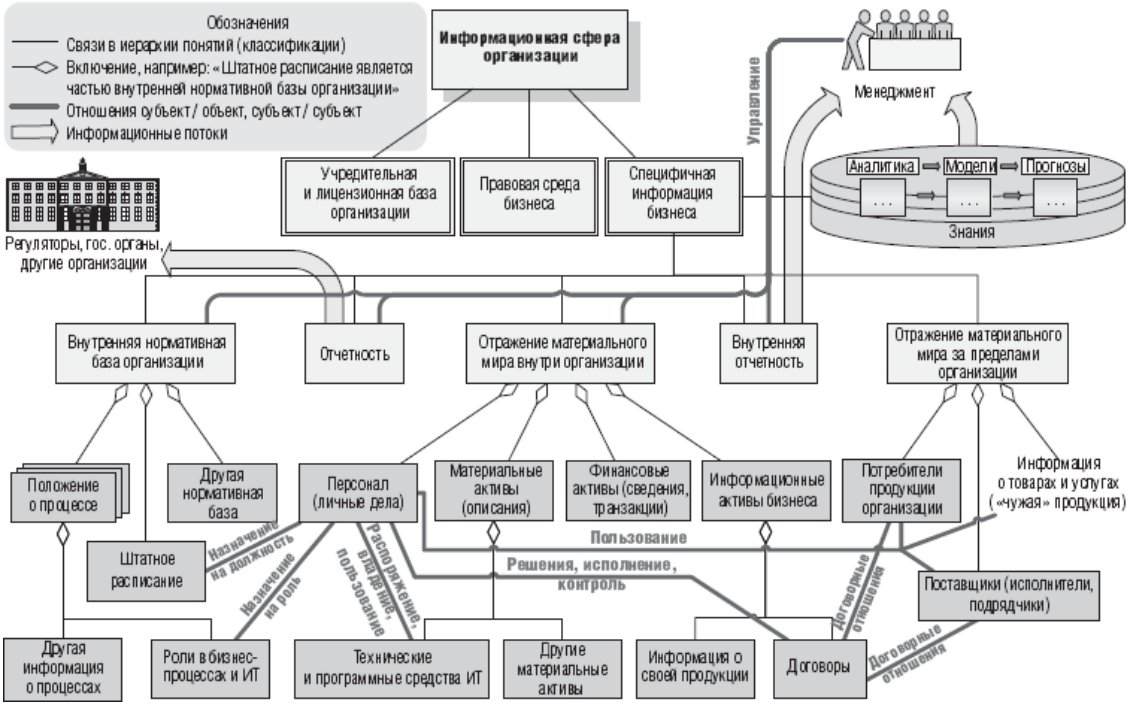

Рис. 4. Структура информационной сферы организации

Внешняя отчетность перед государственными органами (например, налоговая отчетность), регуляторами и другими организациями регулируется нормами правовой среды и, в некоторых случаях, договоренностями между организациями: партнерами по бизнесу, представителями одной отрасли и т. п. Основная проблема, связанная с внешней отчетностью – обеспечение ее соответствия требованиям законодательства или установленным правилам и договоренностям. Как правило, организации стремятся выполнить предлагаемые требования с минимальными затратами и с учетом используемых мер контроля со стороны организаций, которым отчеты готовятся. Если отсутствуют механизмы контроля, то не следует ожидать адекватного отображения действительного положения вещей в подотчетной организации. В этих случаях внешняя отчетность может быть инструментом информационного противоборства и способствовать получению преимуществ в бизнесе. Информационное воздействие состоит в формировании правдоподобных отчетных данных, не полностью или в искаженном виде отражающих внутреннее состояние и деятельность подотчетной организации. Особенно это касается отчетности для партнеров по бизнесу.

В нижней части рис. 4 приведен перечень видов информационных объектов. Совсем необязательно, чтобы любые объекты этих видов хранились в виде компьютерных баз данных или файлов. Это могут быть и бумажные документы, и даже просто договоренности между субъектами, например владельцами бизнеса, но все равно это остается информацией. Вопрос лишь в том, насколько эта информация приспособлена для автоматизированной обработки, какие следы остались на материальных носителях, имеет ли эта информация юридическую силу.

Отметим также, что информация разных видов, приведенных на рис. 4, не является статичной. Каким-то образом должна поддерживаться ее актуальность и адекватность материальному миру. Некоторые виды информации меняются медленно, например информация по персоналу. Другие, наоборот, постоянно изменяются, отслеживая состояние реальных объектов. Критичными для бизнеса являются изменчивые объекты, поскольку именно они – потенциальный источник неадекватностей, а также могут создавать риски разной природы и разной значимости для достижения целей деятельности.

Рассмотрим подробнее особенности отдельных компонентов информационной сферы.

1.2.2. Правовая среда бизнеса и ее свойства

Правовая среда бизнеса включает постановления правительства, законодательные и нормативные акты федерального уровня и уровня регуляторов, региональные законы и нормы, отраслевые стандарты и правила и прочие документы. Наличие обязательного к исполнению набора требований и правил, включая отчетность по нормам правовой среды, является своеобразной движущей силой, организующей и упорядочивающей бизнес, порой определяющей внутреннюю структуру организаций, некоторые виды деятельности и правила поведения участников бизнеса. Эта правовая среда также во многом определяет основу для внутренних нормативных документов организации.

Однако зачастую на уровне конкретной организации не удается избежать формального подхода к обеспечению соответствия законодательным актам. Деятельность, определяемая требованиями правовой среды, остается только на бумаге в виде планов и в большей или меньшей степени фиктивных отчетов, позволяющих удовлетворить потребности государственных проверяющих и регулирующих органов при получении лицензий и плановых проверках. Это может рассматриваться как элемент информационного противоборства и позволяет организации получить преимущество в бизнесе, уменьшая свои расходы на соответствующую инфраструктуру и вследствие этого не вполне соответствуя требованиям, отраженным в формально полученных лицензиях и сертификатах. Информационное воздействие состоит в предъявлении этих лицензий и сертификатов, навязывающих клиентам и другим участникам бизнеса неполную, искаженную, но правдоподобную информацию.

Важное негативное свойство правовой среды бизнеса – неполнота и противоречивость законодательной и нормативно-правовой базы. Это обеспечивает широкое поле деятельности по поиску возможностей и разработке схем для получения преимуществ в бизнесе, от незначительных, на первый взгляд, пунктов в договорных документах, влекущих за собой ущербы одной из сторон, которые трудно или невозможно предсказать (информационное противоборство), до разрушения целей других участников бизнеса и хищения чужих знаний через переманивание сотрудников.

Наконец, еще одно важное свойство – большой объем информации правовой среды, затрудняющий поиск решений, оптимальных с точки зрения успешности бизнеса и соответствия законодательству.

1.2.3. Учредительная и лицензионная база организации

Каждая организация в зависимости от ее формы собственности должна иметь набор учредительных документов. Состав и содержание этих документов определяются требованиями национального законодательства. При этом довольно значительная часть существенных для деятельности требований должна быть установлена (выбрана) самой организацией (ее собственниками) из предлагаемых законодательством возможностей. Эти документы должны быть зарегистрированы установленным порядком и постоянно актуализироваться при возможных изменениях. Де-факто деятельность организации может не совпадать с заранее декларированной, что может порождать коллизии. Поэтому на временные интервалы актуализации в законодательстве наложены ограничения, требующие дополнительной регистрации (перерегистрации) в установленный срок.

В случае если декларируется вид деятельности, подлежащей лицензированию, то такая лицензия должна быть получена в соответствующем органе заранее, до начала осуществления деятельности. Лицензия, как правило, выдается на определенный, достаточно короткий срок и

должна возобновляться. Кроме того, она вообще может быть отозвана при выявлении, например, фактов реализации деятельности с нарушениями требований лицензии. При значительном количестве лицензий в организации она фактически постоянно будет вынуждена находиться в состоянии их актуализации, документировать и подготавливать необходимые активы и свои возможности для их анализа со стороны лицензирующей организации. Эта деятельность связана в широком смысле с комплаенс-риском (риском соответствия требованиям законодательства) для организации.

1.2.4. Отражение материального мира

Существенная часть информационной сферы, относящейся к информации бизнеса, является просто отражением материального мира. Внутри организации это описание ее активов, отношений и их типов, данные мониторинга бизнес-среды и собственной среды и др. Например, материальные и финансовые активы и их движение учтены в базах данных бухгалтерии и складов, персонал также учтен в базах данных бухгалтерии (зарплата, командировочные и др.) и отдела кадров (личные дела, графики отпусков, результаты оценок исполнительской деятельности и др.). Технические и программные средства, инструменты, используемые в информационных технологиях организации, учитываются, как правило, в базах данных конфигурационных единиц. Материальная ответственность работников за используемые в производстве средства и материалы также зафиксирована в соответствующих базах. Отношения работников зафиксированы в иерархической структуре организации (штатное расписание) и в виде функциональных обязанностей ролей и взаимодействий, определенных для реализуемых организацией технологических процессов, сервисов, услуг.

За пределами организации материальный мир включает описания товаров и услуг (продукции), необходимых для реализации ее бизнес-процессов, поставщиков продукции (исполнителей, подрядчиков), потребителей продукции, производимой самой организацией (заказчиков), и отношений с поставщиками и потребителями. Информация о товарах и услугах извлекается разными путями: с использованием каталогов и рекламных материалов поставщиков, из средств массовой информации, Интернета, от дилеров, агентов и других представителей поставщика, от торгующих организаций и т. п. Информация о производимой продукции размещается в аналогичных источниках. Отношения с поставщиками и потребителями закрепляются в соответствующих договорах.

С отображением материального мира в информации связаны две существенные проблемы:

– неточность отображения материального мира на информационный мир, следующая из принципиальной невозможности точного описания объектов материального мира;

– неизменность информационных объектов во времени, позволяющая говорить о том, что время, как естественная сущность, в информационном мире отсутствует и может поддерживаться только искусственным путем.

Любой информационный объект, представляющий материальный, в некотором смысле является моделью этого материального объекта, т. е. описывает лишь существенные для конкретной операции или транзакции свойства материального объекта. Таких описаний для разных целей может быть несколько. Соответственно, информационных объектов, представляющих материальный, также будет несколько, и храниться они, скорее всего, будут в разных местах. Сбор необходимых сведений о материальном объекте из совокупности информационных источников может представлять собой сложную задачу. Рассмотрим для примера информацию о корпоративном сервере.

– Информация о текущей конфигурации аппаратных средств сервера должна храниться в базе данных конфигурационных единиц организации (если такая существует), а также в базах учета материальных ценностей (активов), в бухгалтерских платежных документах, в договорах на выполнение пусконаладочных работ и прочих документах. Причем если конфигурация изменялась, например, оборудование докупалось, то, чтобы установить текущую конфигурацию, например, по бухгалтерским данным, надо восстановить историю закупок.

– Конфигурационные файлы с настройками операционной системы и приложений хранятся в дисковой памяти самого сервера. Эта информация также может быть продублирована у системных администраторов, обслуживающих сервер, если есть соответствующий регламент, в резервных копиях и других местах.

– Информация о фактически сделанных резервных копиях носителей и отдельных файлов хранится в регистрационных журналах сервера, т. е. на сервере, а также вместе с резервными копиями. Кроме этого, должно существовать действующее расписание резервного копирования и регламент, устанавливающий допустимые интервалы копирования.

– Информация о дежурном системном администраторе, обслуживающем сервер, может быть извлечена из графика дежурств, имеющегося в обслуживающем подразделении. Поскольку график дежурства может нарушаться по разным причинам, то, чтобы установить, кто фактически обслуживает сервер в настоящий момент или в другое интересующее время, скорее всего, потребуется брать справку в диспетчерской службе, обслуживающем подразделении или даже в отделе кадров или другой службе учета.

– Еще сложнее получить информацию о том, кто использовал сервер, т. е. был авторизован на нем, и какие имел права на доступ к его ресурсам.

Этот список может быть продолжен, но и перечисленного, на наш взгляд, достаточно, чтобы понять проблему и возможные сложности со сбором нужных данных, например, при необходимости провести расследование инцидента.

Все это усугубляется проблемами, связанными со временем. Первая проблема состоит в том, что информационный образ материального объекта или события есть моментальный снимок, отделенный (отчужденный) от объекта. Он не меняется с течением времени, в то время как объект естественным образом стареет и может подвергаться разного рода модификациям. В результате нарушается адекватность информационного образа самому объекту.

Вторая проблема со временем состоит в том, что, если описания некоторых событий или объектов не снабжены специальной информацией, так называемыми метками времени, то, как правило, восстановить последовательность событий или последовательность состояний объектов по их информационным представлениям невозможно. Например, в файловых системах операционных систем обычно предусмотрена регистрация времени последнего обращения к файлу и времени последней модификации. Чтобы учесть последовательно появляющиеся версии файла, а также кто и когда проводил модификацию и осуществлял доступ, необходимо использовать специальные системы. Это системы учета версий, используемые при разработке программного обеспечения, или специализированные системы регистрации событий (системы мониторинга), применяемые службами информационной безопасности.

Все перечисленные проблемы отражения реального мира в информацию фактически я разные стороны одной проблемы – обеспечения адекватности информационных образов реальным объектам и событиям материального мира. При этом важнейшим является вопрос организации информации. Используемые информационные структуры должны обеспечивать возможность сбора необходимых данных в заданные сроки и с необходимым качеством.

1.2.5. Внутренняя нормативная база организации

Внутренняя нормативная база организации имеет иерархическую структуру, вариант которой показан на рис. 5. Высокоуровневые документы определяют общую политику организации по разным вопросам. Положения, определенные в документах верхнего уровня, раскрываются и детализируются в ряде документов нижних уровней, воплощаясь в конкретные требования, регламенты и т. п. Самый нижний уровень документов – свидетельства выполненной деятельности – определяет возможности по контролю деятельности организации в целом, ее составных частей и персонала.

Рис. 5. Структура нормативной базы

В идеале нормативная база организации должна снимать все неопределенности, которые могут возникнуть в процессе какой-либо деятельности, реализуемой внутри организации, с определением возможных свидетельств выполненной работы и показателей, характеризующих ее качество. Однако это недостижимо хотя бы потому, что, как рассмотрено выше, не существует точного отображения материального мира в информационный. Хорошая и достаточно полная нормативная база организации делает бизнес упорядоченным и прозрачным, а деятельность детерминированной и хорошо контролируемой.

Любые неопределенности, т. е. слабо регламентированная деятельность, порождают риски возникновения потерь и других негативных последствий, из которых наиболее опасен конфликт интересов. Изменчивая внутренняя среда организации, плохо организованная, неадекватная информационная сфера, коллизии и противоречия, возникающие из слабо регламентированной, а следовательно, плохо контролируемой деятельности, приводят к тому, что персонал организации при определенных условиях может использовать порученные ему для управления активы для извлечения личной выгоды.

Когда деятельность осуществляется в области, где не установлены правила и отсутствуют регламенты, то можно либо замотивировать любые необходимые для нецелевого управления активами полномочия, либо просто выполнять любые действия с ними, мотивируя их впоследствии тем, что они были необходимы для выполнения заданной работы, за которую сотрудник отвечает. В этих случаях обнаружить, что персоналом были выполнены какие-то неправомер-

ные действия, можно только по косвенным признакам и, как правило, с задержкой по времени. Предъявить какие-либо доказательства этих действий невозможно. Доказать, что у конкретного сотрудника был злой умысел, также нельзя. А поскольку потери все равно есть всегда, то понять, какая их часть была вызвана манипулированием (фальсификацией) информационными активами, а какая обусловлена естественной природой бизнеса и величиной его стохастичности, бывает трудно. Стохастическая составляющая бизнеса не может быть проверена, и очень плохо, если она большая в силу самой природы бизнеса.

Поскольку структура некоторой части внутренней нормативной базы организации во многом определяется правовой средой бизнеса, то еще один источник неопределенностей внутренней нормативной базы связан с неполнотой и противоречивостью правовой среды бизнеса.

Слабая внутренняя нормативная база, т. е. неполная и противоречивая, приводит к необходимости опираться на доверие персоналу. Высокий уровень изменчивости внутренней и внешней среды бизнеса, т. е. большая стохастическая составляющая самого бизнеса, также требует, чтобы собственник в большой степени полагался на доверие персоналу и партнерам по бизнесу.

1.2.6. Информационная сфера – главный источник рисков бизнеса

Рассмотренные аспекты бизнеса, связанные с информацией и информационной сферой, позволяют сделать вывод, что информационная сфера является одним из главных источников рисков бизнеса. Подведем итог и еще раз выделим основные свойства или факторы, способствующие появлению этих рисков.

Возрастающая сложность. В настоящее время наблюдается резкий рост количества факторов, влияющих на успешность бизнеса, и их пространственно-временная распределенность. Основной причиной этого роста является резкий рост количества субъектов экономической деятельности в мире, и в особенности в России. Количество связей растет квадратично. Как следствие, растет и информационный компонент бизнеса, поскольку для успешности бизнеса, не говоря даже о повышении его эффективности, необходимо учитывать все большее число факторов. Это приводит к необходимости создания информационной инфраструктуры с соответствующими техническими и программными средствами.

Сложность информационной сферы многократно усиливает действие других факторов риска и порождает уязвимости, вызванные дефицитом времени на обработку и осознание вариантов возможных решений, невозможностью проверки достоверности всех используемых данных. Дополнительные риски связаны с использованием и поддержанием информационной инфраструктуры, технических и программных средств обработки данных, компьютерных сетей и телекоммуникаций.

Неточность отображения материального мира в информационные образы (модели). С этим связана проблема обеспечения адекватности информационных моделей, участвующих в обработке данных и прогнозах, реальным объектам. Выше отмечались две проблемы:

– неточность отображения материального мира на информационный мирнеизменность информационных объектов во времени, порождающая со временем неадекватность информационного образа реальному объекту.

Поскольку действия над материальными объектами во все большей степени замещаются действиями над их описаниями (информационными образами), то неадекватность этих описаний приводит к коллизиям, из которых наиболее значимы два крайних случая:

– отсутствие информационного образа для реально существующего объекта, который мог бы быть использован в бизнесе;
– наличие информационного образа для объекта, реально не существующего.

Теоретическая возможность коллизий подобного рода порождает риск их искусственного создания (уничтожение данных об объекте, изъятие объекта), приводящего к ущербу и потерям. Однако и без злоумышленных действий неадекватность информационных образов (моделей) объектов самим материальным объектам создает значительные риски, особенно на этапах целеполагания и планирования. Поэтому обеспечение адекватности является самостоятельной задачей и не должно осуществляться стихийно, по фактам необходимости в использовании той или иной информации.

Конфликт интересов. Все более сложные образования из субъектов разного уровня и отношения, возникающие между ними, в условиях, что цели у всех них разные, создают в результате конфликт интересов. Острота этой проблемы увеличивается из-за резкого увеличения количества взаимодействий. Можно выделить два взаимосвязанных между собой уровня конфликта интересов:

– внутри организации (внутренний конфликт интересов);
– между организациями.

Внутренний конфликт интересов – один из главных источников риска и главная угроза бизнесу, поскольку в этом случае персонал организации и особенно субъекты ответственности и высший менеджмент используют в своих интересах активы организации, включая информацию, материальные и финансовые активы и другие ресурсы. При увеличении размеров организации конфликт интересов тоже резко усиливается просто из-за того, что очень много субъектов оказываются вовлеченными в процессы как внутри, так и снаружи организации.

Это не только объективное свойство любого бизнеса, но и основа механизма его самоуничтожения. Накопление избыточного ресурса в подразделениях больших организаций приводит к резкому снижению эффективности бизнеса. Использование этих избыточных активов для своих целей, не совпадающих с целями организации, и создание при помощи информационных воздействий, таких как искажение отчетности, ослабление контроля, маскировка причин неудач под естественную случайность и других, иллюзии, что бизнес реализуется нормально и эффективно, приводит в конце концов к потере управления, крупным неудачам, ущербам и ликвидации бизнеса. Искусственно создать условия, благоприятные для внутреннего конфликта интересов, и, как следствие, ухудшить бизнес может и информационная атака извне.

Конфликт интересов между организациями – это, как правило, конкуренция и борьба за общий ресурс, например клиентов. Острота проблемы конфликта интересов между организациями усугубляется при увеличении количества взаимодействий. Реализуя свой бизнес, приходится учитывать большое количество факторов, и здесь неизбежно возникает конфликт интересов.

Проблема доверия. Проблема доверия возникает там, где отсутствуют или существенно неполны механизмы контроля. Внутри организации – это проблема доверия собственников персоналу организации, и в первую очередь руководству и менеджменту верхнего уровня. Для тех видов бизнеса, где велика стохастическая составляющая и в силу этого контроль просто невозможен, остается полагаться на доверие. В других же случаях к необходимо-

сти полагаться на доверие приводит слабость внутренней нормативной базы и, как следствие, слабо регламентированная, а следовательно, плохо контролируемая деятельность.

Причина и необходимость полагаться на доверие и устные договоренности в отношениях между организациями следуют из неполноты и противоречивости законодательной и нормативно-правовой базы (правовой среды) бизнеса и, как следствие, невозможности контроля исполнения партнерами по бизнесу и конкурентами законодательно установленных правил.

Проблема доверия состоит в том, что если кто-то нарушит некие правила, то он получит большие преимущества. У партнеров по бизнесу и конкурентов в связи с этим возникают существенные риски потерь или даже ликвидации бизнеса. Очевидно, что в условиях возрастающей сложности, наличия и обострения конфликта интересов, неадекватности информационной сферы риски, связанные с доверием, возрастают, а преимущества, получаемые субъектом и организацией, нарушающими правила могут быть очень большими.

Проблема информационной безопасности состоит в том, чтобы организация могла использовать информационную сферу на всех этапах своего жизненного цикла в реализуемых ею видах бизнеса, в условиях угроз, связанных с перечисленными выше проблемами и особенностями. По сути это некие технологии, позволяющие эффективно использовать информационную сферу в условиях перечисленных проблем и особенностей. Информационная безопасность существует в рамках некоторых моделей, рассматриваемых ниже.

1.3. Модель информационной безопасности бизнеса

1.3.1. Мотивация

Российская и мировая практика регулирования информационной безопасности (ИБ) недавнего прошлого состояла из обязательных требований национальных уполномоченных органов, оформляемых в виде руководящих документов РД. Поэтому для топ-менеджмента и владельцев организаций существовала только одна проблема соответствия им (комплаенс) и только один способ ее решения – как с минимальными затратами выполнить предлагаемые требования. Для уполномоченных органов существовала своя проблема – как в силу невозможности охвата всех возможных видов деятельности и условий их реализации, а также существенных различий в целях деятельности предложить универсальный набор требований. Для этого проблема ИБ рассматривалась как самодостаточная сущность, инвариантная к деятельности, целям, условиям, а также существенно обуживалась в содержательности в угоду универсальности.

Оба подхода (организаций и регуляторов) неадекватны существующей реальности и представляют ее в существенно искаженном виде. Так, основные содержательные ограничения на деятельность по обеспечению ИБ связаны с традиционной моделью ИБ, предполагающей обязательное наличие злоумышленника, стремящегося нанести ущерб активам (информации), и, соответственно, ориентированной на защиту информации от действий такого субъекта (группы субъектов). При этом инциденты, связанные, например, со штатными изменениями прикладного софта, не могут быть отнесены к злоумышленнику. Их возможные причины – слабо развитый менеджмент и слабая технологическая база. Собственная неадекватность организации (менеджмента, процессов основной деятельности) сложившимся условиям вообще представляет собой очень мощный источник проблем, который игнорируется в силу невозможности его привязки к злоумышленнику.

Дальнейшая эволюция моделей ИБ была связана с усилением роли собственника (владельца) и сводилась к тому, что он сам выбирал (на свой страх и риск) из предложенного ему стандартного набора защитных мер те, которые ему необходимы, т. е. такие, которые, по его мнению, могут обеспечить приемлемый уровень безопасности. Это был существенный шаг вперед, так как он обеспечивал привязку ИБ к конкретному объекту с конкретными условиями его существования, частично разрешая противоречия, связанные с самодостаточностью проблемы ИБ. Однако конструктивного механизма для владельца предложить не удалось, кроме как создания каталога объектов с выбранными типовыми защитными мерами (профилей защиты). Сами профили создавались при этом экспертно-эвристическим методом. При этом какой все-таки риск принимал на себя владелец, оставалось неизвестным и определялось на практике.

Дальнейшая эволюция свелась к тезису о том, что ИБ может создавать (порождать) ущербы для целей деятельности и поэтому риски ИБ (которая оставалась самодостаточной) должны быть согласованы (увязаны) с рисками организации. Оставалось только указать, как их увязывать, и интегрировать систему менеджмента ИБ (СМИБ) в общекорпоративный менеджмент не как изолированную и независимую систему процессов, а как неотъемлемую, сильно связанную составную часть менеджмента. Этого не удалось сделать. Однако этот подход хорошо продвинул ряд оценочных категорий ИБ, включая риски ИБ.

Известны также прагматичные модели ИБ, основанные на оценке совокупной стоимости владения (применительно к ИБ) и «возврате» инвестиций в ИБ. В рамках этого подхода группа близких по целям и условиям деятельности организаций периодически производит

оценку по направлениям реализации ИБ и формирует модель, состоящую из лучших практик по группе. Далее каждая из организаций в соответствии со своими отставаниями от лучших практик и своих условий (произошедших инцидентов) определяет направление и объем инвестиций. Эффективность инвестиций оценивается в следующем периоде по снижению ущербов от инцидентов, оказавшихся в области произведенных инвестиций и не повлекших поэтому больших ущербов.

Однако этот подход при многих своих достоинствах требует широкого обмена чувствительной информацией, а конфликт интересов участников обмена исключает создание сколько-нибудь качественных мер доверия, поэтому он не имеет широкого распространения.

Модель ИБ, предложенная в стандарте ЦБ РФ, еще более продвинула проблему как в части ее интеграции (связала с целями деятельности), так и в части расширения толкования сущности «злоумышленник». Под злоумышленником понимается лицо, способное вести противоборство с собственником и имеющее свою цель, которую он реализует, достигая контроля над активами организации.

Такой подход существенно расширяет виды и источники ущербов организации, попадающих в область рассмотрения ИБ, где их решение наиболее рационально. Он, однако, был во многом компромиссным подходом и настоятельно требует дальнейшего приближения проблем ИБ к конечному результату деятельности (производимому продукту). Нужна модель, которая реально помогает бизнесу, напрямую способствует его результативности и необходимому улучшению посредством создания и поддержания безопасной и доверенной информационной сферы, в том числе через борьбу со злоумышленником. Только такая модель может восприниматься бизнесом. Любая другая будет им отторгаться.

1.3.2. Риски, рисковые события, ущербы и уязвимости. Полезные для построения моделей свойства

Любая целенаправленная деятельность связана с неопределенностью конечного результата, порождающей риск. Риск реализуется через рисковые события, создающие ущерб целям деятельности. Рисковое событие есть следствие сложившегося неблагоприятного сочетания факторов риска, т. е. некоторых сущностей и (или) обстоятельств, являющихся существенными для проявления риска. Таким образом, фактор риска можно рассматривать как его параметр, принимающий нежелательное (неблагоприятное) значение, а рисковому событию соответствует некоторый набор таких параметров. Следовательно, говоря о риске, мы предполагаем как минимум, что наших знаний достаточно, во-первых, для идентификации риск-факторов, а во-вторых, для их измерений (оценки).

Легко заметить, что риск можно уменьшить, создав избыточность по всем задействованным сущностям. Однако его нельзя сделать нулевым, даже если создать бесконечно большую избыточность. Дело в том, что нельзя сформулировать цель на бесконечно большом интервале времени – в силу изменчивости среды она теряет смысл. Кроме того, составляющая риска, обусловленная изменчивостью условий реализации целей, является неуправляемым фактором.

Как только мы создаем избыточность, уменьшающую риск, мы одновременно уменьшаем эффективность деятельности. Последнее обстоятельство важно для бизнеса – одной из основных разновидностей процесса целенаправленной деятельности. Проблема установления рационального баланса между эффективностью и безопасностью есть главная проблема бизнеса. Это информационная проблема. Ее решение потребует знаний.

Таким образом, первичным является вопрос о способности накапливать и обобщать знание и понижать тем самым степень неопределенности результатов деятельности. Накопление знаний – эволюционный многоаспектный процесс обобщения своего и чужого опыта в конкретных условиях деятельности. Последовательно развивая и усиливая свое знание, мы сна-

чала научимся идентифицировать происходящие изменения в системе влияющих факторов; затем, сопоставляя их с наступившими последствиями, мы научимся их (факторы) оценивать; потом, пытаясь избежать негативных последствий, мы научимся правильно (адекватно) реагировать на изменения риск-факторов. И наконец, на основе анализа причинно-следственных связей и отношений между состояниями процесса целенаправленной деятельности и достигаемыми результатами идентифицировать новые факторы влияния.

В связи с этим для нас состоянием процесса целенаправленной деятельности будет состояние уже идентифицированных факторов риска. Иные состояния, находящиеся ниже «уровня видимости», не могут быть нами учтены. Для идентифицированных факторов часть состояний будет нами различаться, но пока в связи с невозможностью еще их оценивания будет временно игнорироваться и направляться для обобщения в процедуру накопления знаний.

Процесс целенаправленной деятельности может менять свое состояние, и смена состояния является событием. Это, однако, не рисковое событие, которое наступает, только когда все обуславливающие его риск-факторы принимают «неблагоприятные» значения и приводят к ущербу. Поэтому реально рисковому событию предшествует временной ряд простых событий, связанных с изменением значений риск-факторов. Эти события могут интерпретироваться как рисковые события, зависящие от изменившихся факторов, но не способные нанести ущерб. Часто их различают, называя рисковое событие, повлекшее ущерб, инцидентом.

Разные факторы обладают разной степенью изменчивости, есть быстро изменяющие состояние, есть медленно. В случае, когда группа медленно изменяющихся факторов установилась в неблагоприятное состояние, можно говорить о том, что в процессе целенаправленной деятельности сложилась рисковая ситуация. Выделение рисковых ситуаций практически существенно упрощает процедуры анализа и оценки рисков и принятие решений по ним. Примерами рисковых ситуаций могут быть ситуации, связанные с персоналом (невозможно быстро переобучить или заменить персонал на более компетентный); с операционной средой (невозможно одномоментно сменить большой объем компьютеров) и т. д.

Природа рисков такова, что одно и то же рисковое событие может порождать разные по видам и величине ущербы. Как это уже было указано, ущербы характеризуются неопределенностью и зависимостью от факторов, определяющих состояние процесса целенаправленной деятельности. Можно указать на практически полную аналогию величины возникающего ущерба с рисковыми событиями с точки зрения его возникновения, анализа и оценки. Однако ущерб рассматривается как условная сущность (при условии, что рисковое событие произошло), а влияние выделенных факторов величины ущерба рассматривается на практике с учетом естественной способности процесса противостоять рисковым событиям. Такое свойство процесса называется защищенностью или обратной ей сущностью уязвимостью (более распространено) процесса к рисковым событиям определенного вида.

Другой особенностью представления ущерба факторной моделью является то, что описывается потенциально возможный ущерб. Реальный ущерб определяется парой «потенциально возможный ущерб, уязвимость». Уязвимость, таким образом, может быть определена на практике по соотношению возможного ущерба и реального ущерба. При этом если потенциальный ущерб большой, а реальный маленький, то уязвимость мала, и, наоборот, если реальный ущерб близок к возможному, то уязвимость большая.

Риск-ориентированный подход к целенаправленной деятельности существенно трансформирует понятие «злоумышленник». Оно расширяется, поскольку наличие «злого умысла» уже не является основным признаком деятельности субъекта, приводящей к инциденту. Для организации важно и опасно, когда деятельность субъекта (ов) вне зависимости от его (их) намерений порождает (увеличивает) риск для ее целей. Это обстоятельство является основой для своевременной идентификации рисковых событий. Наличие умысла в действиях субъекта

может быть установлено в дальнейшем в ходе расследований, и это является важным с точки зрения правильного (адекватного) реагирования на возникающую проблему.

Понятно, что речь идет только о субъекте, действующем в области внутренних (управляемых) факторов риска. Если субъект действует в стохастической области бизнеса (в области внешних неуправляемых факторов), то возникновение связанных с его деятельностью рисковых событий неизбежно, и контроль (оценка) деятельности такого субъекта возможен только по ее конечному результату.

Противодействовать возникновению рисковых событий – значит своевременно их идентифицировать и осуществлять компенсационные воздействия на риск-факторы, в том числе и на постоянной основе с помощью защитных мер. При этом основная задача – не допустить одновременного действия критического сочетания риск-факторов.

1.3.3. Обобщенная модель распределения ресурсов организации в условиях рисков

Основное содержание любого бизнеса – управление ресурсами в пространстве и времени для достижения цели. Не претендуя на построение общей модели бизнеса, которая могла быть использована для практических целей, таких как его улучшение, увеличение прибыли и т. п., рассмотрим некоторую сильно упрощенную (обобщенную) модель управления ресурсами организации, применимую для целей анализа влияния ИБ на бизнес, и, как следствие, лучшего понимания места и роли ИБ в организациях. Основными особенностями бизнеса являются:

а) привлекаемый (используемый) ресурс для достижения цели (производства продукта, предоставления услуги) приобретается в общем случае на заемные средства;

б) производимый продукт реализуется на рынке, и выручка, полученная в ходе реализации, есть источник покрытия всех издержек.

Будем считать, что бизнес осуществляется в виде двух операций: заем, инвестирование – и характеризуется временем реализации цели $T_{Ц}$. Под целью понимается своевременный возврат заемных средств и получение прибыли в результате реализации продукта, произведенного за счет инвестирования заемных средств. При этом предполагается, что кроме заемных средств собственник (организация), осуществляющий бизнес, располагает собственными средствами в виде некоей совокупности активов, часть из которых ликвидная.

Заем характеризуется объемом $\tilde{V}_{Z}$, платой за заем $П_Z$, интервалом времени возврата T_Z. Пусть $V_Z = \tilde{V}_Z + П_Z$. Тогда заем есть пара $<V_Z, T_Z>$.

Инвестиция характеризуется объемом $\tilde{V}_{И}$, временем возврата инвестиций $T_И$, величиной возврата инвестиций $\tilde{V}_{P}$. Цель любого инвестирования – вернуть больше, т. е. выполнить соотношение $\langle \tilde{V}_P > \tilde{V}_И \rangle$.

Будем считать бизнес сходимым, если возврат инвестиций осуществлен в большем объеме, чем заем и все остальные издержки, т. е. если $\Delta V = \tilde{V}_P - V_Z > 0$. При этом время $T_Ц$ реализации цели не столь критично, как время T_Z возврата заемных средств.

Вследствие того, что только параметр T_Z является фиксированным, а остальные параметры процесса подвержены рискам различной природы, может оказаться, что на момент возврата инвестиций $\Delta V < 0$. Возникающая коллизия может быть покрыта в конечном счете только из собственных средств организации, ее способность разрешать такие коллизии является рисковой категорией.

Рассмотрим последовательно некоторые виды возникающих рисков. По факторам, от которых они зависят, их можно разделить на две группы:

– неуправляемые риски, полностью определяемые внешними факторами – в первую очередь рыночные риски $R_р$;

– управляемые или частично управляемые риски, зависящие от внутренних и внешних факторов.

На управляемые риски организация может влиять, проводя соответствующие мероприятия, и влияние тем сильнее, чем больше доля внутренних факторов, от которых зависят риски. Для упрощения рассмотрения ограничимся пока тремя видами рисков этой группы: стратегическим $R_{стр}$, операционным $R_{оп}$ и ликвидности $R_{л}$.

С учетом рыночного риска объем возврата инвестиций (реализации) $\tilde{V}_р$ может оказаться как меньше, так и больше ожидаемого объема $V_Р$. В худшем случае – меньше. С учетом рыночного риска $\tilde{V}_р = V_р - V_{рр}$, где $V_{рр}$ – убыток от реализации, привносимый рыночным риском. При отрицательном убытке получим, что $\tilde{V}_р > V_р$. Аналогичным образом рыночный риск влияет на время реализации, привнося дополнительное время $\Delta T_{Рр}$, которое может быть как положительным, так и отрицательным.

Для покрытия издержек от реализовавшихся рисковых событий организация должна либо иметь страховой фонд (резерв капитала), либо уметь быстро реализовывать часть своих активов для получения недостающих средств. Собственно, страховой фонд (резерв капитала) – это тоже актив.

Страховой фонд может быть создан за счет заемных средств. При условии, что рисковые события реализовались, фактические инвестиции увеличатся на величину ущербов, полученных от реализовавшихся событий стратегического и операционного риска. Оценка риска до начала инвестиций позволяет спрогнозировать эти потери. Объем инвестиций с учетом возможных потерь будет включать

$V_И = V_Z + V_{Zстр} + V_{Zоп}$, (1)

где $V_{Zстр}$, $V_{Zоп}$ – резервы на предполагаемые потери, связанные со стратегическим и операционным рисками соответственно.

Действия по реализации части активов могут быть направлены на формирование фонда резервирования основного капитала организации, при этом важнейшими показателями являются свойство ликвидности этого резерва и объем резерва.

Связанный с реализацией части актива риск $R_л$ называется риском ликвидности. На этот риск влияют три фактора: $V_Л$ – объем ликвидных активов, $C_Л$ – стоимость этих активов и $T_Л$ – время их реализации. Из них $V_Л$ по сути есть характеристика структуры (количества и характера) активов – внутренний (управляемый) фактор организации, а $C_Л$ и $T_Л$ – это внешние факторы, зависящие от величины рыночного риска.

Таким образом, существует система рисков, воздействующих на объемные (V_i), временны́е (T_i) параметры либо на оба типа параметров (V_i, T_i) одновременно. Связи рисков с параметрами иллюстрируются рис. 6.

Каждая организация идентифицирует свои риски достижения заявленных целей. Выявленная в результате идентификации рисков система рисков есть риск-ориентированная модель организации, определяющая условия достижимости ее целей деятельности.

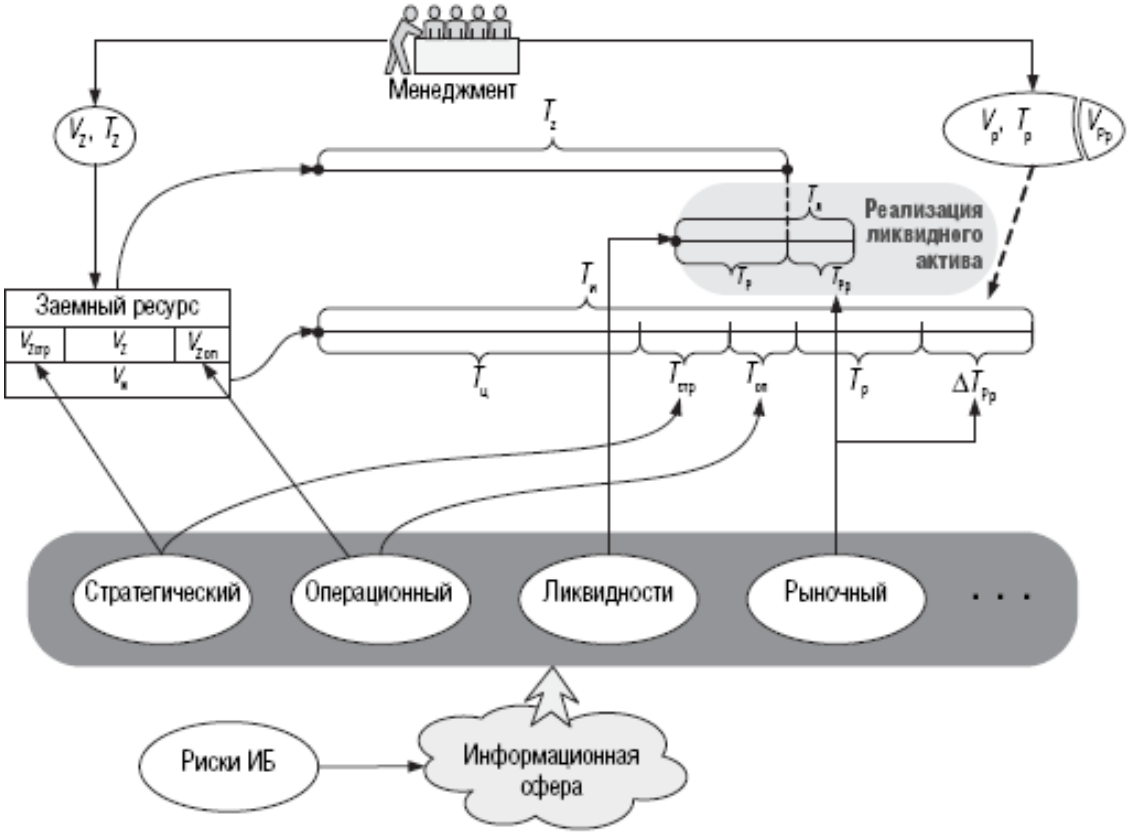

Рис. 6. Обобщенная модель распределения ресурсов организации в условиях рисков

С точки зрения проблемы ИБ часть идентифицированных рисков, имеющая отображение на информационную сферу организации, образует базис, используемый далее для построения модели ИБ организации, отражающей причинно-следственные связи и отношения между рисками ИБ и рисками для целей деятельности организации. Сами идентифицированные риски для целей деятельности организации, образующие базис, будем называть базовыми.

1.3.4. Ущербы и негативные последствия

Ущерб – это сложная, многоаспектная сущность. На вид и величину ущерба, помимо материальных составляющих, влияют социальная, нравственная и культурная составляющие, степень зрелости гражданско-правового общества и государства, а также индивидуальные предпочтения отдельно взятого субъекта и то состояние, в котором он находится в данный момент времени. В интересующем нас смысле можно рассматривать два вида ущерба:

а) ущерб субъекта как категория системы гражданско-правовых отношений, связанных с какой-либо реализуемой деятельностью;

б) ущерб субъекта как категория права на реализацию какой-либо деятельности.

Ущерб в пункте а) определяется в контексте гражданского, административного, уголовного кодексов РФ, а также соответствующими процессуальными кодексами, регулирующими процедуры инициирования сбора свидетельств, расследования и рассмотрения в суде связанных с ущербами споров. Очевидно, что чем более развита и совершенна эта система, то тем более широко (полно) и тем более точно определяет она возможные виды ущербов и способов их оценивания.

Для нас важным является то обстоятельство, что мы рассматриваем только подмножество ущербов, наступивших в связи со злоупотреблением (фальсификацией) информационной сферы, и этот факт должен быть установлен и подтвержден. В связи с тем, что отношения «субъект, субъект» и «субъект, объект» есть информационные сущности, равно как и цели, которые мы стремимся достичь в процессе осуществляемых деятельностей, область влияния информационной сферы на субъектов, механизмы и степень этого влияния весьма обширны и многообразны.

Основной результат этого влияния – некачественно реализованная цель, снижающая ожидаемую выгоду от ее реализации. Это может иметь разное выражение (отображение). В бизнесе – уменьшение получаемого дохода как в прямом смысле, так и через увеличение различных издержек, прямых и косвенных потерь (объемных и стоимостных), задействованных в реализуемых деятельностях активов, удовлетворения различного рода претензий, связанных с неисполнением (некачественным исполнением) принятых обязательств, и т. д.

Принципиальным является то обстоятельство, что все не идентифицированные в терминах гражданско-правовой сферы негативные последствия для субъекта деятельности могут быть отнесены только на него самого (сам виноват). Кроме того, может оказаться, что регулируемые гражданско-правовой сферой негативные для субъекта последствия обеспечивают неадекватное реальному ущербу возмещение. Эта часть ущерба также относится на субъекта деятельности.

Таким образом, потенциальный объем ущербов, приходящихся на субъекта (доля в общем объеме негативных последствий), большой. Естественно, что он, предпринимая различные меры, стремится его уменьшить.

Любой субъект деятельности в процессе реализации своих целей может не только нанести ущерб сам себе, но и другим (или ему другие наносят ущерб), а также ущерб может быть нанесен государству. Такой ущерб обусловлен тем, что субъекты взаимодействуют не только между собой, но и с государством (в том или ином виде), а у государства есть не только права, но и обязанности. Государство может нести ущерб не только в сфере своих прямых обязанностей, но и в виде различных компенсаций субъектам, не сумевшим разрешить свои конфликты интересов (коллизии) в рамках гражданско-правовой сферы. Кроме того, государство может быть ответчиком в суде и проиграть по искам. Эта практика растет.

Минимизируя свои риски, государство совершенствует гражданско-правовую сферу, частично перенося тем самым свои риски на взаимодействующих субъектов. Кроме того, через уполномоченных органов-регуляторов государство вводит различные системы ограничений и отслеживает их исполнение субъектами деятельностей. Ограничения могут вводиться и непосредственно в виде законов. Можно выделить, хотя бы условно, два направления ограничений:

а) требования (ограничения) на качество производимого продукта (услуги);
б) ограничения на способ реализации деятельности (технологию).

Очевидно, что прежде всего государство стремится минимизировать риски в зоне своей прямой ответственности: общественная, экономическая и иные виды безопасности; безопасность жизнедеятельности и т. д. Однако, вводя, например, экологические ограничения на бизнес, государство может увеличить нагрузку на бизнес и уменьшить свою нагрузку.

Понятно, что ограничения, предъявляемые к качеству продукта, естественным образом отображаются в гражданско-правовую сферу, так как качество продукта есть один из предметов взаимодействия участвующих субъектов.

Другое дело – ограничения в способе реализации деятельности. В общем случае потребителю продукта или услуги все равно, каким образом он был произведен. Поэтому для бизнеса такого рода ограничения есть дополнительные издержки, увеличивающие затраты и понижающие эффективность деятельности. Понятно, что если в совокупности такого рода издержек будет много, то бизнес станет неэффективным (убыточным) и будет свернут. Особенно плохо, когда ограничения на деятельность выражаются в виде некоторой обязательной технологии. Тогда субъект, сумевший решить проблему лучше и дешевле, все равно будет нарушителем, и к нему будут применены соответствующие санкции.

В любом случае понятие ущерба и негативных последствий в рассматриваемой нами проблеме является фундаментальным и первичным. Если изначально понятие «ущерб» не формализовано как с точки зрения идентификации, так и оценки величины, то все дальнейшие рассуждения о его минимизации и избежании останутся умозрительными и вряд ли перейдут в практическую плоскость.

1.3.5. Риск-ориентированный подход к обеспечению ИБ

В общем случае риски определены на множествах факторов, влияющих на них. Эти множества могут пересекаться. Если от некоторого фактора зависят два или более рисков, то эти риски оказываются взаимозависимыми. Их значения будут коррелированны, поскольку изменение общего для них фактора приведет к одновременному изменению этих рисков. Эта ситуация иллюстрируется рис. 7, где в области факторов показаны пересекающиеся множества управляемых и неуправляемых факторов, от которых зависят разные виды рисков.

Особенностью риска ИБ является то, что он зависит от большого количества факторов, множество которых в общем случае пересекается с множествами факторов, от которых зависят практически все другие риски (см. рис. 7). Поэтому хотя риск ИБ непосредственно не влияет на V_i, T_i, но в силу взаимозависимостей с другими рисками оказывается с ними сильно коррелированным. Это свойство проявляется в дальнейшем в реализующихся в процессе деятельности организации рисковых событиях.

Из всех рисков риски ИБ наиболее сложные по своей природе, имею т самую большую неопределенность как по рисковым событиям, так и по наносимому ущербу. Факторные модели рисков ИБ поэтому имеют большую размерность и разнообразные причинно-следственные связи и отношения по сравнению с другими рисками.

Так, например, событие операционного риска «Отказ сервера», происшедшее вследствие влияния факторов физической природы, значительно более предсказуемо, чем отказ как следствие влияния человеческого фактора злонамеренной природы. Лежащий в основе такого события конфликт интересов описывается несопоставимо более сложной факторной моделью, чем факторная модель надежности сервера.

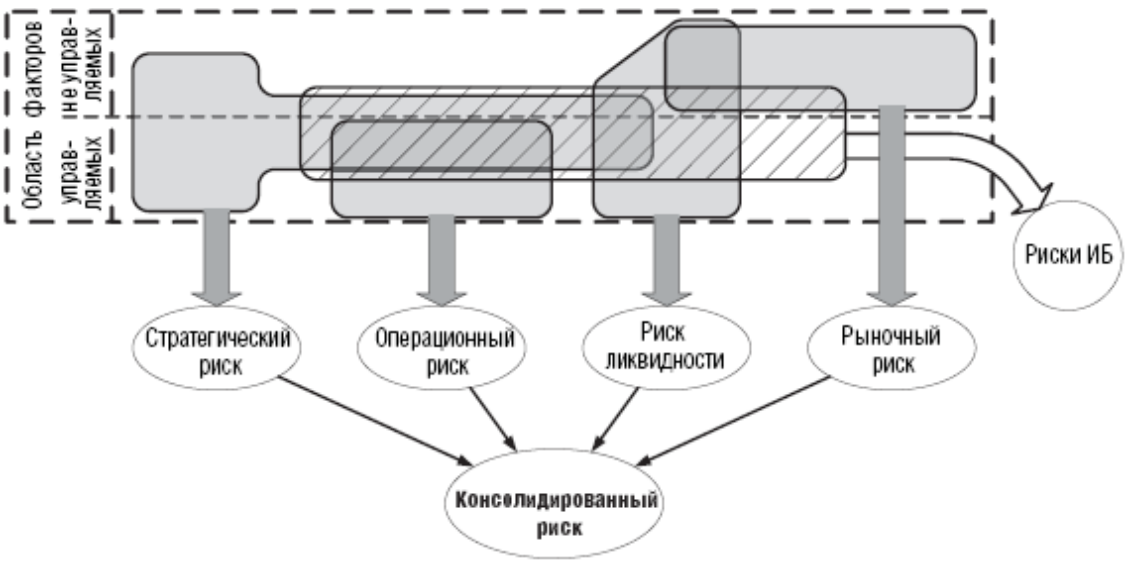

Рис. 7. Коммуникативность и взаимозависимость базовых рисков

Именно поэтому «типовой сценарий» значимого рискового события ИБ (повлекшего значительный ущерб) сводится, как правило, к тому, что реализуется пачка событий (временной ряд) с незначительным ущербом (часто вообще без ущерба); в результате влияния пачки создается и удерживается некоторое время рисковая ситуация и, как следствие, реализуется значимое рисковое событие.

Иными словами, особенностью рисковых событий и ситуаций ИБ является то, что они протяженные во времени и накапливающегося типа, т. е. любое событие в отдельности наносит очень (на практике пренебрежительно) малый ущерб, вследствие чего они игнорируются. При этом независимо от того, реагируем мы на эти мелкие, с небольшим ущербом инциденты или нет, если их происходит много, то накапливается некий «негативный потенциал», порождающий в конце концов крупный инцидент. Эта особенность может быть в некоторых случаях содержательно объяснена, например злоумышленник может порождать множество мелких инцидентов в процессе подготовки к атаке при исследовании атакуемой системы. Тогда инцидент с большим ущербом будет результатом успешно проведенной атаки.

Если абстрагироваться от каких-либо возможных причин, лежащих в основе накопления «негативных потенциалов», то в качестве гипотезы можно рассматривать *принцип накопления «негативного потенциала»от пачки инцидентов*. Этот принцип подтверждается реально существующей статистической структурой инцидентов. В приближенном виде эта статистика такова, что существует относительно большое количество мелких инцидентов, создающих незначительный ущерб, на некоторое количество таких мелких приходится один крупный инцидент, существенно превосходящий мелкие по масштабам, и есть особо крупные инциденты, возникающие реже крупных и также существенно превосходящие их по масштабам ущерба.

Статистическая структура инцидентов неизменна для каждой организации и слабо зависит от видов ее деятельности и целей деятельности. Параметры структуры могут быть установлены через историю (прошлое организации), если она зафиксирована. Предположительно число мелких инцидентов на два порядка больше крупных, а ущерб от одного крупного инцидента как минимум на порядок больше ущерба от всех мелких, приходящихся на него. Особо крупные инциденты возникают на три-пять крупных и превосходят их или сравнимы с ними по масштабам ущерба.

В конце пачки инцидентов риск скачкообразно изменяется до очень больших значений. Из принципа накопления также следует, что влияние событий ИБ на организацию зависит от

ее состояния, от того, какие значения базовых рисков сложились к моменту возникновения событий ИБ. Одно и то же событие ИБ может дать различный эффект – от незначительного ущерба до катастрофического. Если говорить об общей характеристике рисковых событий ИБ, то это провоцирующие (создающие условия) события для базовых рисков организации.

Таким образом, рисковые события ИБ всегда «вложены» в базовые риски бизнеса (организации) и проявляются в виде ущерба, который организация идентифицирует как ущерб, связанный с базовым риском. Тот факт, что понесенный ущерб был инициирован проблемами информационной сферы, не всегда рассматривается, а реагирование на риск осуществляется методами, присущими базовыми рисками (экономическими, финансовыми, юридическими и др.). Часто это существенно менее эффективные и более затратные способы реагирования, чем информационные.

Очевидно, что для более осмысленного и качественного реагирования на базовые риски организации необходимо отобразить на них информационную сферу организации. Однако прямое отображение информационной сферы на базовые рисковые события либо крайне затруднительно, либо вообще невозможно. Причина этого разрыв как семантический, так и формальный, а также и временно й между содержанием и формой представления событий в информационной сфере организации и конечным продуктом (целью) ее деятельности.

Менеджмент организаций, как показывает практика, более склонен воспринимать возникающие издержки как последствия сложившихся разного рода ресурсных ограничений, но не информационных. Однако та же практика, только a posteriori, каждый раз показывает, что дело было вовсе не в ресурсных ограничениях, а сводилось к тому, насколько эффективно организация была способна добывать полезную для себя информацию, оценивать и систематизировать ее, анализировать, накапливать, обобщать, а также своевременно и рационально использовать в своей деятельности. Без эффективно действующей информационной составляющей даже изначально ресурсно избыточный бизнес погибнет.

Поэтому построение модели ИБ организации должно начинаться с исследования (анализа) идентифицированных в ней рисков целей деятельности (бизнеса). Целью этого анализа должно быть установление контекста идентифицированных рисков, т. е. определение условий, сущностей и механизмов реализации рисковых событий, вида и величины наносимого ущерба.

Установленный контекст позволит перейти к построению факторных моделей базовых рисков, т. е. к некоторой их формализации, приближающей их к сущностям информационной сферы. При этом факторы и обстоятельства, слабо связанные с процессами информационной сферы, могут сразу же отфильтровываться как незначимые.

Одновременно необходимо формализовывать и информационную сферу в контексте базовых рисков организации. Такое движение навстречу позволит преодолеть указанный выше разрыв. Наилучшей основой такой формализации является технологический аспект, т. е. отображение на нее ролей и субъектов, а также задействуемые ими активы и инструменты (информационной сферы).

Теперь можно установить контекст информационной сферы для идентифицированных риск-факторов, т. е. какие активы, процессы, инструменты, субъекты и роли отображаются на каждый из риск-факторов. Здесь же, если уже накоплено достаточно знаний, устанавливается, какие именно нарушения (регламентов, свойств либо состояния) являются признаками (либо предвестниками) наступления событий ИБ. Последующий мониторинг этих сущностей позволит идентифицировать часть событий ИБ.

Именно пятерка «активы, процессы, инструменты, субъекты, роли» (далее «А, П, И, С, Р») подвержена рискам ИБ, и происходящие с ними события ИБ будут приводить к изменению значений соответствующих риск– факторов и, как следствие, значений базовых рисков организации и ее совокупного риска.

Видно, что пятерка «А, П, И, С, Р» определяет содержательно и формально критическую часть информационной сферы организации, способную наносить ущербы и приводить к негативным последствиям для целей организации. Таким образом, у базовых рисковых событий всегда через их риск-факторы может быть идентифицирован их контекст в информационной сфере организации.

Понятно, что если пересечение контекстов событий S_i и S_j не пустое, т. е. $K\langle S_i\rangle \cap K\langle S_{ij}\rangle \neq \varnothing$, о между S_i и S_j возникает связь и можно говорить о связанной цепочке событий. Можно также говорить о силе этой связи, понимая под ней значение $A_{ij} = K\langle S_i\rangle \cap K\langle S_j\rangle \neq \varnothing$, т. е. чем больше A_{ij}, тем сильнее связь.

Еще более сильной характеристикой связи является понесенный ущерб (негативные последствия) и его информационный контекст. В этом смысле можно говорить о событии «понесенный ущерб», связанном с обнаружением факта ущерба. Здесь важна величина ущерба V и по аналогии с событиями базового риска идентифицированная с ним пятерка «А, П, И, С, Р».

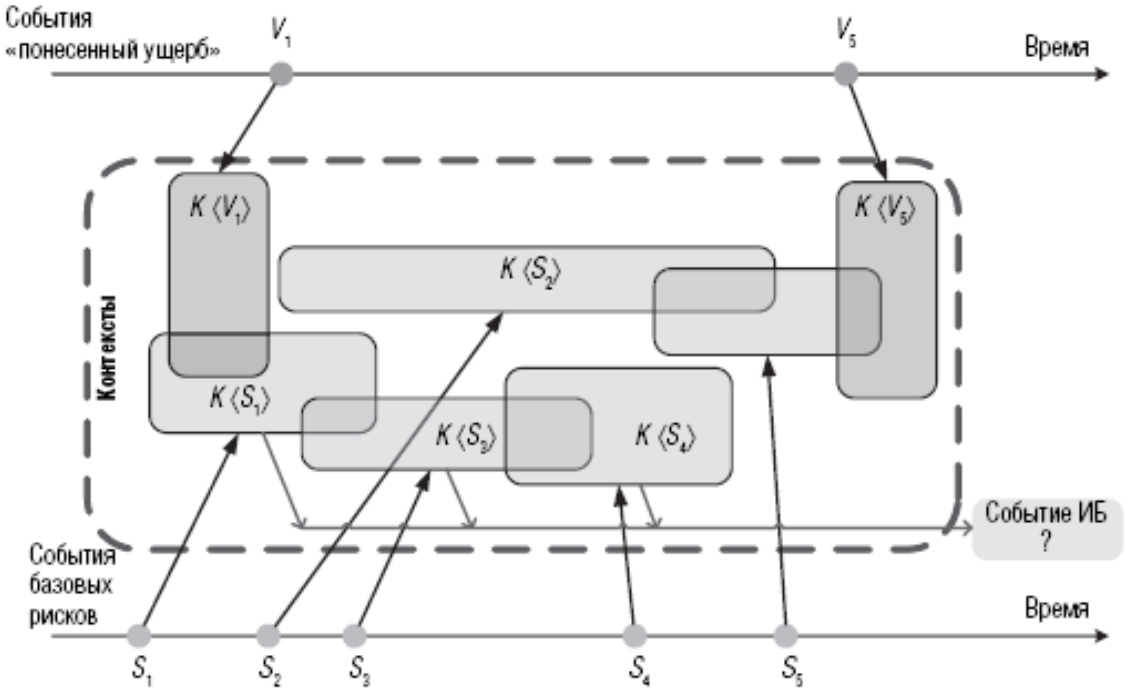

Рис. 8. Контекстная зависимость событий базовых рисков

То есть с точки зрения безопасности более важно не само рисковое событие, а наступившие последствия, их оценка (величина) и идентифицированный контекст, в нашем случае в терминах информационной сферы. Связи рисковых событий и понесенных ущербов иллюстрируются рис. 8. Связи событий могут быть неочевидны, особенно в случае понесенных ущербов и событий базовых рисков. В общем случае они устанавливаются в результате расследования. Понятно, что идентифицированная таким образом цепочка с сильными связями будет отображать цель и примененный способ ее реализации для нанесения ущерба.

Описанные выше процедуры установления контекста базовых рисков организации в ее информационной сфере и «связывания» их с событиями ИБ являются основой построения модели ИБ организации. Однако практическая их реализация требует более детального рассмотрения проблем идентификации событий ИБ, управления ИБ, систематизации, оценива-

ния, анализа и обобщения получаемой информации о состоянии организации (бизнеса) и ее информационной сферы. Эти вопросы рассматриваются ниже.

1.3.6. Модель с изменением цели

Рассмотренная выше модель основывается на неизменности достигаемой цели. Однако одной из распространенных мер реагирования на риск является корректировка (деградация) изначально заявленной цели. В ситуации, когда инвестиционный процесс реализуется последовательно (часто это естественный процесс), можно определить прогнозные оценки конечного результата, т. е. величину ΔV. При $\Delta V \geq 0$ процесс следует считать нормальным и можно перейти к дальнейшему инвестированию.

В ситуации, когда на очередном шаге окажется, что $\Delta V_i < 0$, необходимо осуществить корректировку цели так, чтобы ΔV_i (Ц – $Ц_i$) ≥ 0, где $\tilde{Ц}_i = Ц - Ц_i$ – величина корректировки цели на шаге i. Ограничив возможности по корректировке цели так, что $\tilde{Ц} = \sum_{i=\overline{1,n}} \tilde{Ц}_i < \delta,$ где δ – допустимая величина корректировки цели, получаем итерационный процесс реализации цели в контексте рассмотренной выше модели. Процесс завершается либо после завершения всех шагов инвестирования ($i = n$, n – количество шагов инвестирования), либо при достижении $\tilde{Ц} > \delta.$ Тогда оставшиеся шаги ($n - i$) реализуются за один шаг инвестирования.

Понятно, что возможности по изменению цели ограничены не только условной величиной δ, но и особенностями (свойствами) самой цели. Корректирующие возможности существенно обуживаются при увеличении объемов инвестирования: на первых шагах они больше, а к последнему шагу эти возможности очень ограничены.

Поэтому нужна некоторая стратегия, учитывающая это обстоятельство. Риски такой стратегии связаны с точностью прогноза величины $\Delta V_i, i = \overline{1,n}$ и возможностью точного ее покрытия корректировкой цели. Ошибки этих прогнозов накапливаются к последним инвестиционным этапам.

1.3.7. Об идентификации событий ИБ

Задача идентификации событий ИБ состоит в выявлении событий ИБ среди полного множества различных событий организации. Трудности идентификации событий ИБ связаны с их косвенным влиянием на базовые риски организации (бизнеса), а также с тем, что отдельные (одиночные) события ИБ в силу их слабого влияния могут быть и вовсе не идентифицированы как события ИБ. Причина этого в том, что риски ИБ проявляются в наступлении событий иных (базовых) рисков. Так, например, отказ сервера (событие операционного риска) может иметь злоумышленную природу, и тогда это событие ИБ. Здесь видно, что почти всегда напрямую факторы рисков ИБ отображаются только на участвующего субъекта в виде факторов его совокупного объема знаний, мотивов, возможностей.

Под идентификацией рисковых событий ИБ будем понимать выявление среди общего потока событий в информационной сфере тех событий, которые прямо или косвенно (в сочетании с другими событиями) приводят к негативным последствиям для бизнеса.

Вследствие указанных выше обстоятельств идентифицировать напрямую рисковое событие как событие ИБ практически всегда невозможно. Исключением являются рисковые собы-

тия, прямо связанные с работой средств защиты, например зафиксированные в регистрационных журналах попытки НСД. В остальных случаях это будут события базовых рисков, например операционного риска. Квалифицировать эти события как события ИБ (или инциденты ИБ) можно только по результатам расследования.

Тем более сложно оценить с точки зрения влияния на бизнес идентифицированное одиночное событие ИБ. Поэтому должна быть предложена система критериев как по идентификации, так и по оценке событий ИБ. Можно указать на ряд значимых факторов, обусловливающих возникновение событий ИБ:

а) неполная, недостоверная и несвоевременная внутренняя отчетность в организации и связанный с ней конфликт интересов: участвующие субъекты не заинтересованы в предоставлении отчетности, ухудшающей их статус в организации;

б) наличие стохастической составляющей (областей неформализованной деятельности), исключающей какие-либо формы контроля за деятельностью;

в) несовершенство ролей, ответственностей и организационных политик в организации и связанная с ними инсайдерская деятельность;

г) злоумышленная активность персонала;

д) противоборство организации за заимствуемые ресурсы с внешними субъектами;

е) организационное, функциональное и информационное несовершенство информационной сферы организации;

ж) слабости менеджмента в части накопления, обобщения, применения опыта для достижения целей организации;

з) неспрогнозированные изменения негативно влияющих факторов внешней среды, которые привели к увеличению базовых рисков.

Ситуация усугубляется тем, что значительная часть злоумышленников думает вовсе не о нанесении ущерба организации, а только о своей выгоде, и тем, что их деятельность может наносить ущерб третьим лицам, а не организации напрямую; может влиять негативно на какой-нибудь консолидированный показатель типа эффективности деятельности, наступление ущерба от которого солидарно распределяется между всеми участвующими субъектами, что крайне затрудняет идентификацию.

Совершенно понятно, что любой субъект, создающий для своей организации проблемы ИБ, будет препятствовать своей идентификации, создавая (или используя) различные неопределенности. Для этого у него есть целый ряд возможностей. Например, он может:

а) действовать в рамках чужих либо «ничьих» полномочий (ролей);

б) найти в рамках своих штатных полномочий различные непредусмотренные дополнительные возможности и их использовать;

в) исследовать структуру деятельности организации, обнаружить там условия возникновения коллизии (когда все действуют штатно, но возникает событие ИБ) и их инициировать в нужное ему время.

Самый простой и понятный способ идентификации событий ИБ основывается на предварительном анализе и фильтрации всех контролируемых в организации событий по принципу предопределенности в интерпретации события. Например, события, связанные с выявлением проникновения и тем более запуском вредоносного программного кода (вирусов). Очевидно, что иных целей, кроме злоумышленных, тут не может быть. То же можно сказать и о любых нарушениях в используемых технологиях на основе секрета (PIN-коды, пароли, криптографические ключи и т. д.). Нарушения в этой сфере могут содержать признаки злоумышленной

активности. Можно указать также на процессы и технологии, связанные с отчуждением информации или получением прав доступа к ней, и на процедуры (процессы) контроля информации (особенно прикладными системами). Например, отбраковка первичного документа приложением «1С-Бухгалтерия» может указать на признаки злоумышленной активности при создании этого документа.

Сформированное таким образом подмножество типов данных дает весьма полезную для безопасности информацию. Однако:

а) это очень незначительная часть реально нужной информации;

б) могут быть проблемы с ее доступностью, достоверностью, полнотой и своевременностью.

Дело в том, что в большинстве случаев на практике непосредственное участие безопасности в этих проблемах ограничено созданием нормативной базы. Практическая реализация, а тем более контроль за деятельностью есть предмет соглашения заинтересованных субъектов. В каждой организации это реализуется по-разному, и безопасность лишь частично задействована.

Так, антивирусные средства почти всегда находятся во владении ИТ-подразделения; технологии с применением секрета могут быть замкнуты на бизнес-подразделения организации (в силу причин юридической ответственности исполнителя); контроль сосредоточен, как правило, в системе внутреннего контроля организации. Однако даже эта ограниченная информация уже может дать хороший результат, если обеспечить ее контекстное расширение и использовать накопительный анализ по всему контексту. Для этого для каждого зарегистрированного / задокументированного события необходимо идентифицировать все вовлеченные объекты (активы), процессы, инструменты, субъекты, роли. По всей полученной базе и нужно проводить анализ.

Как еще расширить полезную информацию, по каким критериям?

• На основе анализа расширить область предопределенности, выделив активы, процессы, инструменты, субъекты, роли, существенно влияющие на риск-факторы. Далее для выделенных элементов осуществить накопительный анализ по всем событиям базовых рисков на предмет выявления злоумышленной активности.

• По величине ущерба – если ущерб превысит предустановленный порог, то связанное с ним рисковое событие должно исследоваться на наличие злоумышленной активности.

• На основе анализа непрерывности по пространству и времени информационной сферы организации необходимо выделить точки потенциального разрыва типа: «реальное событие было, но не отобразилось в информационной сфере», «реального события не было, а в информационной сфере отображено» и им подобных. Тогда для любого компонента «А, П, И, С, Р», попавшего в разрыв, дополнив его контекстом, необходимо проводить накопительный анализ по безопасности.

Накопительный анализ основывается на обобщениях, позволяющих выделить состояния (события) – предвестники и события – признаки. Предвестники позволяют понизить риски путем своевременного реагирования. Не менее важна своевременная идентификация событий ИБ, так как наносимый ущерб, как правило, скачкообразно возрастает по завершении логически связанной цепочки событий.

Могут быть использованы статистические критерии на основе выявления неоднородностей. Так, например, пачка однотипных (или близких) событий на коротком интервале времени

и позиционированных тем более на ограниченном множестве в пространстве «А, П, И, С, Р» обязательно будет иметь общую причину и, быть может, злонамеренную.

Существуют две области событий, обладающие максимальной (и примерно одинаковой) неопределенностью:

– стохастическая составляющая бизнеса или эквивалентная ей с точки зрения анализа слабо регламентированная или вовсе нерегламентированная область деятельности;
– штатная (разрешенная) деятельность.

В обоих случаях возможен только прямой контроль за целью деятельности. Он основывается на том обстоятельстве, что цель всегда отображается на множество «А, П, И, С, Р» и образует там некоторое отношение порядка. То есть один и тот же субъект в рамках одной и той же назначенной ему роли реализует каждый раз цель либо одним и тем же, либо близким способом.

Для штатной деятельности соответствующие атрибуты активов, процессов, инструментов, отображающие цель деятельности субъекта и роль, могут быть получены в результате анализа; для неформализованной деятельности – в результате наблюдения за деятельностью и сопоставления ее с полученным результатом. Так получают образец «хорошего». Образец может быть далее формализован (представлен в виде модели), атрибуты могут быть представлены статистически (в виде гистограмм) или, например, ранжировок, а затем агрегированы (консолидированы) в оценку. Эта оценка фактически есть числовое (может быть, и пространственное) выражение (отображение) цели деятельности.

Далее такая метрика может быть использована для фильтрации наблюдаемых событий на периодической основе либо в реальном времени. В последнем случае деятельность рассматривается как временной ряд событий, в котором с помощью модели можно прогнозировать реализацию тех или иных событий. По величине отклонений наблюдаемых событий от наиболее вероятных можно судить о «сдвиге» в цели деятельности. Здесь возможен накопительный анализ, т. е. пачка событий предустановленной длины превысила предустановленный порог.

Анализ на признаки злоумышленной активности проводится для всех пространственно-временных областей деятельности, давших при оценке превышение предустановленных значений цели деятельности. Таким образом, практически все рисковые события (базовых рисков) организации могут иметь злоумышленную природу (с точки зрения ИБ). Отсюда следует, что практически все из них должны исследоваться безопасностью. Однако ясно, что информативность событий существенно разная. Учитывая, что анализ в большинстве случаев накопительный, т. е. размерность задачи большая, становится важным осуществлять этот анализ как можно более целенаправленно. Для этого могут быть использованы два механизма:

– предварительного анализа, позволяющего выявить наиболее информативные с точки зрения ИБ пространственно-временные области деятельности;
– на основе накопления и обобщения реальных практик, т. е. на основе моделей Деминга – Шухарта.

1.3.8. Предварительный анализ

Как видно, влияние рисков ИБ на базовые риски организаций имеет сложный нелинейный характер. Через риски ИБ для базовых рисков происходит консолидация внутренних и внешних риск факторов, что затрудняет оперативный анализ, создает неопределенность. Риски ИБ, реализуясь, искажают (модифицируют) тем или иным способом информационную сферу.

Она, в свою очередь, один из источников (среда) факторов базовых рисков, т. е. некоторая сущность, осуществляющая «перенос» рисков ИБ в базовые риски.

Понятно, что увеличение в силу разных причин числа инцидентов ИБ приведет к увеличению (возникновению) инцидентов базовых рисков, при том что основные влияющие на них риск-факторы не изменились. Возникшее несоответствие есть неопределенность. и классическое реагирование на риск в этом случае будет вынуждено базироваться на противодействии неуправляемым и неизмеряемым внешним факторам, что почти невозможно. Именно поэтому и нужно исследовать, как это указано в задачах идентификации, возможное наличие составляющей безопасности.

По сути, предварительный анализ есть обратная задача идентификации, т. е. мы пытаемся ответить на вопрос о том, какие связи между реализовавшимися событиями ИБ и базовыми рисками и каков их характер. На этой основе априори выделяются критические пространственно-временные области деятельности. Эта неопределенность требует, часто тщательных и трудоемких, расследований, поэтому реальные инциденты ИБ (реализовавшиеся рисковые события) могут быть не закрыты длительное время. Поэтому чрезвычайно важно иметь «заготовки» – предварительно исследованные фрагменты причинно-следственных связей и отношений между вовлекаемыми субъектами и объектами анализа.

Важно также, с какой степенью подробности и достоверности документируются внутренние процессы информационной сферы. Предварительный анализ основывается на тех соображениях, что:

а) рисковое событие есть сочетание активизированных риск-факторов в одной и той же точке, в одно и то же время;

б) наносимый ущерб или наступающее негативное последствие также есть сочетание факторов, определяющих состояние информационной сферы (или бизнеса) и момент времени, когда рисковое событие наиболее опасно. Обычно это бывает на завершающей стадии реализации цели, особенно в случаях, когда произведенные инвестиции будут безвозвратно утрачены.

В этом смысле все возникающие пространственно-временные соотношения и есть предмет анализа. Очевидно, что если поставить риск-факторы в зависимость так, что при активизации одного фактора другой, наоборот, нормализуется, то рискового события не произойдет. Это верно для случая, когда все риск-факторы управляемые, а нормализация приводит к нулевому значению оценки фактора. Если сущности а) и б) сдвинуты во времени так, что при максимальном значении а) наблюдается минимальное значение б), то наступающее рисковое событие не нанесет значимого ущерба.

Конец ознакомительного фрагмента.