В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. Голдуев
Обеспечение информационной безопасности бизнеса

Андрианов В.В
Обеспечение информационной безопасности бизнеса
2-е издание, переработанное и дополненное

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 всё, 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 сообщения 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 передавать 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.

Рис. 2. Качество информации определяет качество и эффективность управления

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.

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.

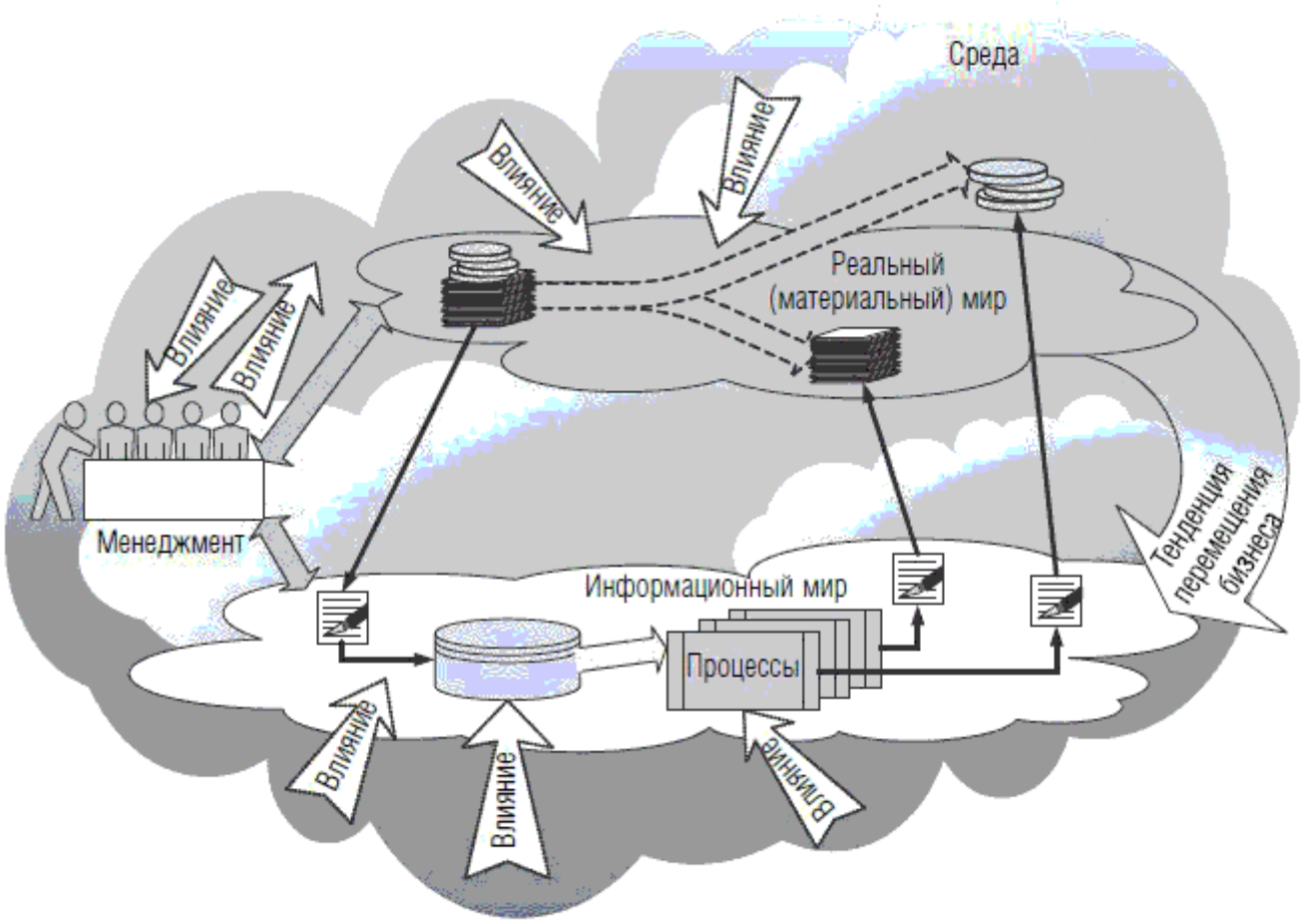


Рис. 3. Взаимодействие материального и информационного миров

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.

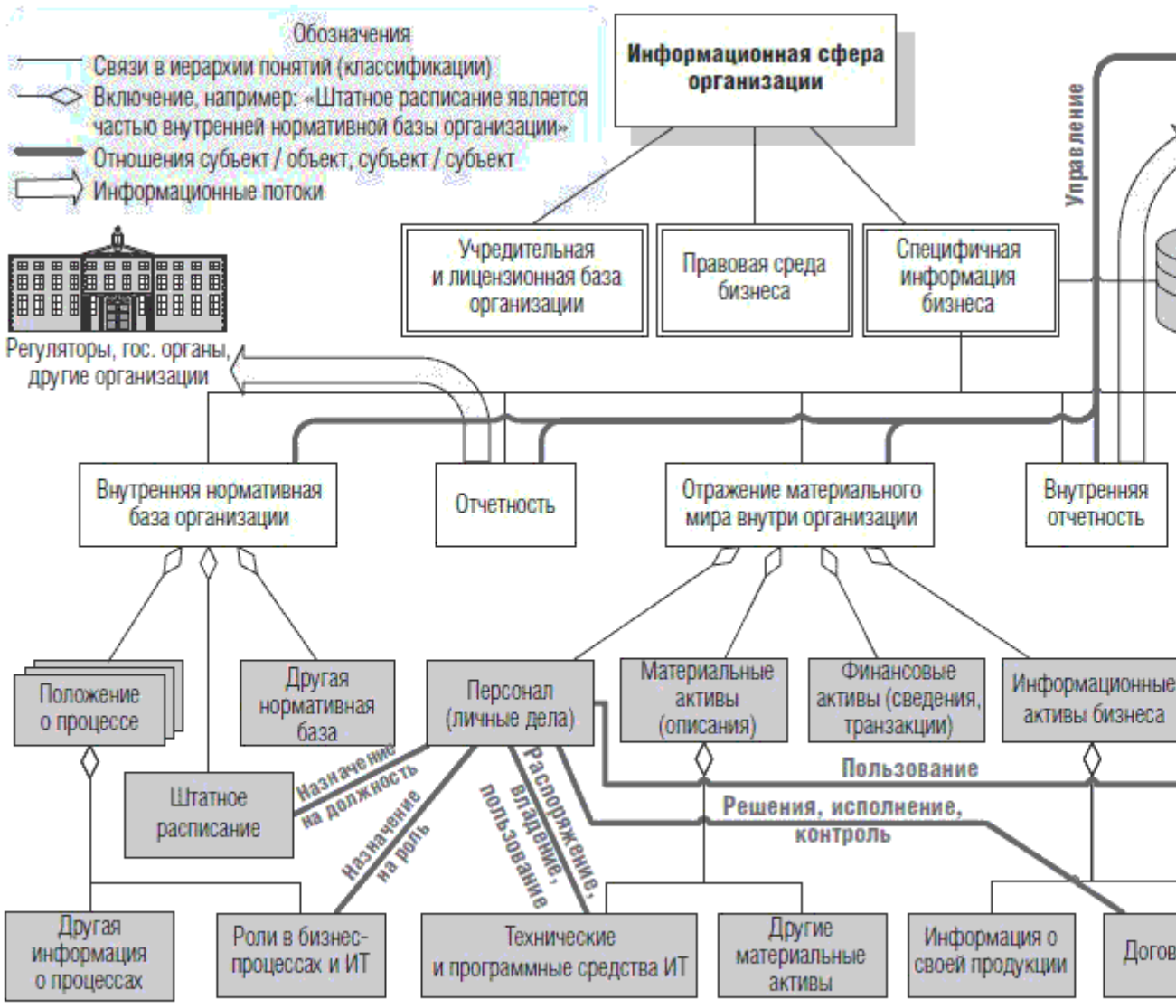


Рис. 4. Структура информационной сферы организации

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.

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 неправомерные 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 необходимости 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 сначала 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 $\widetilde{V}_Z$, платой за заем $П_Z$, интервалом времени возврата T_Z. Пусть $V_Z = \widetilde{V}_Z + П_Z$. Тогда заем есть пара $<V_Z, T_Z>$.

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

Будем считать бизнес сходимым, если возврат инвестиций осуществле в большем объеме, чем заем и все остальные издержки, т.е. есл $\Delta V = \widetilde{V}_Р - V_Z > 0$. 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) $\widetilde{V}_Р$ может оказаться как меньше, так и больше ожидаемого объема $V_Р$. В худшем случае — меньше. С учетом рыночного риска $\widetilde{V}_Р = V_Р - V_{Рр}$, где $V_{Рр}$ — убыток от реализации, привносимый рыночным риском. При отрицательном убытке получим, что $\widetilde{V}_Р > V_Р$. 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

$$V_И = V_Z + V_{Zстр} + V_{Zоп}, \qquad (1)$$

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), временные (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.

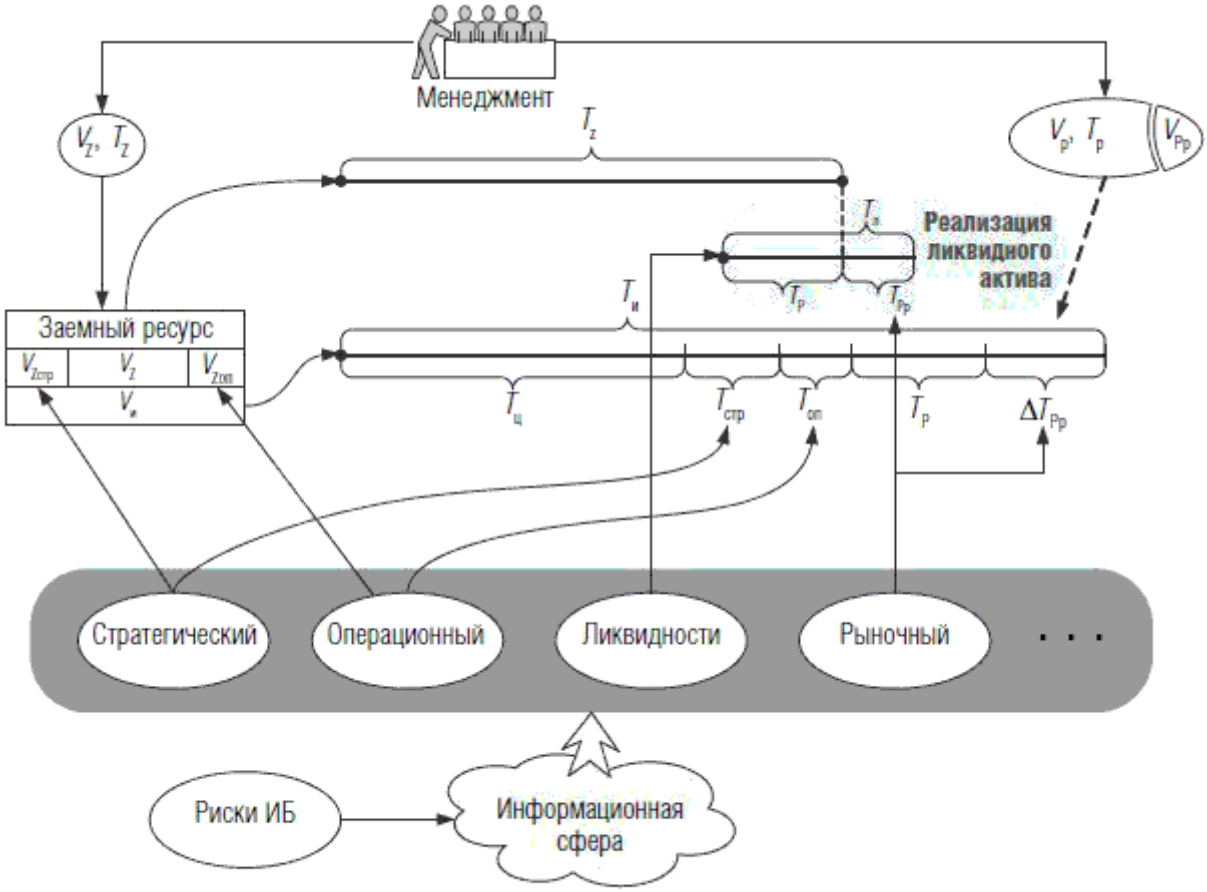


Рис. 6. Обобщенная модель распределения ресурсов организации в условиях рисков

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, имеют 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.

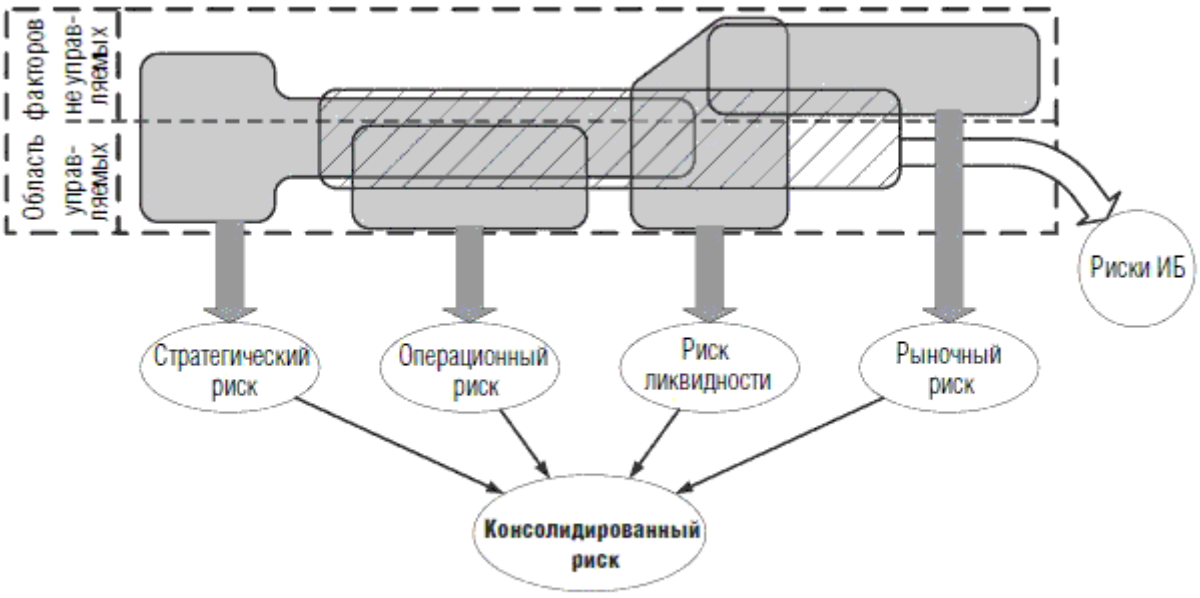


Рис. 7. Коммуникативность и взаимозависимость базовых рисков

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.

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 временнóй 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.

$$K\langle S_i\rangle \cap K\langle S_{ij}\rangle \neq \varnothing,$$

то 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».

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.

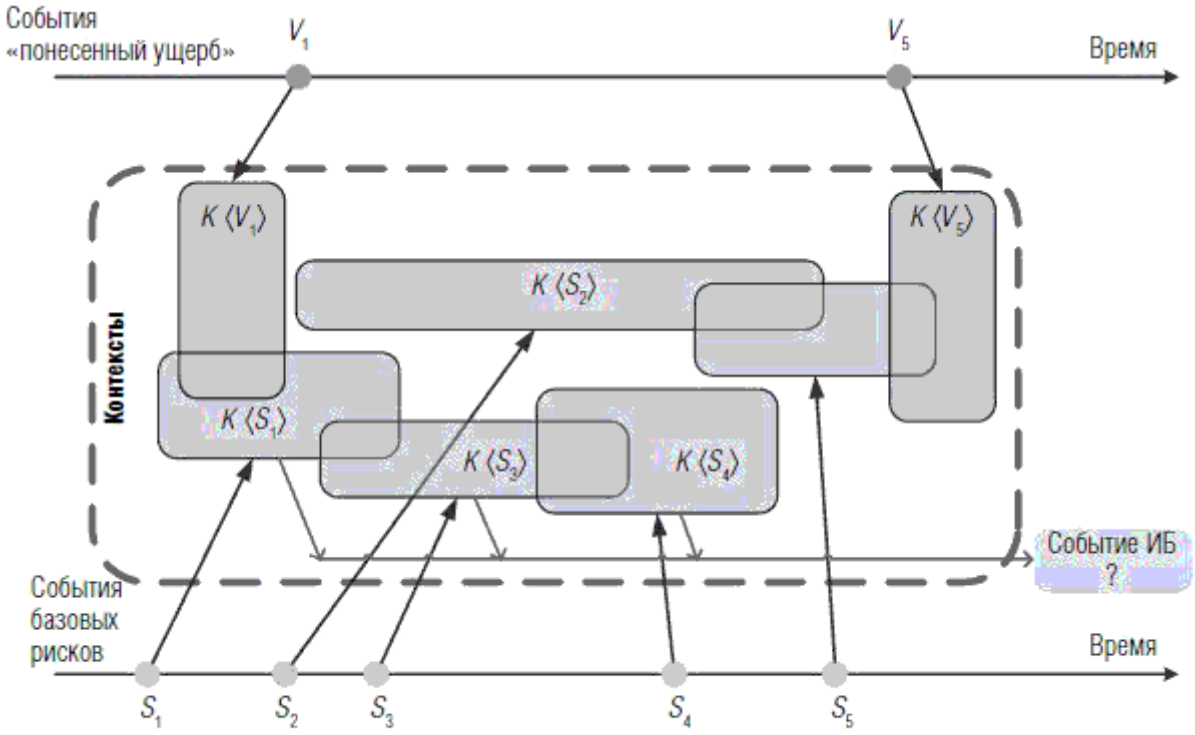


Рис. 8. Контекстная зависимость событий базовых рисков

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, оценивания, 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 $(Ц - Ц_i) \geq 0$, 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 события, 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.

Главная цель анализа – выявить пространственно-временные области деятельности, в которых объект в силу несовершенства своей информационной сферы, своих возможностей и своего поведения сам создает предпосылки (порождает и (или) активизирует факторы) к наступлению событий с потенциально большим ущербом. В таких случаях ущерб списать можно только на «самого себя». В идеале таких случаев не должно быть, они должны быть идентифицированы и устранены.

1.3.9. Накопление знаний

Можно, хотя и достаточно, условно выделить две формы знаний:
– информационное;
– эмпирическое.

Информационное знание получается нами либо умозрительно (на основе анализа и синтеза одних только информационных сущностей без эксперимента), либо вообще в готовом виде извне, например из специальных публикаций по интересующей нас проблеме или от учителя. В последнем случае знание отражает чужой опыт и должно быть принято нами на веру. При этом мы должны ответить на вопрос: если «у них» так было, то почему, в силу каких факторов и обстоятельств, «у нас» будет так же, – понимая при этом, что двух идентичных условий реализации процессов не может быть. Степень нашей уверенности в ответе на поставленный вопрос определяет характеристику такого знания, его силу.

В случае умозрительного моделирования интересующего нас процесса единственным основанием для уверенности может служить тот факт, что «мы уже так делали», хотя и для другого процесса, и с некоторой степенью точности получали полезный результат.

Достоинством информационного знания является то, что это «быстрое» и «дешевое» знание; недостатками – отсутствие исчерпывающих оснований для уверенности в

адекватности этого знания интересующему нас процессу и проблемы с силой такого знания.

Эмпирическое знание, наоборот, основывается только на реальной фактуре, на том, что идентифицированные нами причинно-следственные связи и отношения между объектами и субъектами процесса реально происходили и нами наблюдались в объеме, достаточном для вывода о том, что наблюдаемое нами состояние процесса есть следствие (последствие), и в какой мере, тех или иных произошедших событий. Накопление эмпирических знаний формализуется в рамках модели Деминга – Шухарта, предполагающей определенный цикл шагов, собранных в схему непрерывных циклических улучшений.

В рамках этой схемы мы сначала выдвигаем (формулируем) некоторое предположение о достижимости определенного результата в рамках фиксированного плана деятельности. Реализовав этот план, в общем случае с отклонением реального результата от заявленного, мы подробно исследуем причины несоответствия и вырабатываем корректирующие меры. Процесс продолжается, улучшая предсказуемость достигаемого результата.

Величина несоответствия заявленного и полученного результата в конечном счете зависит от объема использованной информации, глубины и детальности проводимого нами анализа, а также от природы процесса. В ситуации, когда результат в основном зависит от управляемых факторов, предсказуемость будет очень точной, и, наоборот, при зависимости от внешних неуправляемых факторов процесс сойдется на некоторой величине неулучшаемой погрешности. Эту погрешность предсказания (планирования) придется принять и предусмотреть соответствующий резерв для компенсации возможных дополнительных издержек.

Недостаток эмпирического знания – его накопление происходит медленно. Реально это может понижать эффективность деятельности.

На практике используются оба вида знания, причем приоритет должен быть у эмпирического знания как более достоверного (адекватного). Рекомендуемое соотношение для процесса накопления знаний: должно использоваться ~ 30 % чужого опыта (информационное знание) и ~ 70 % своего опыта (эмпирическое знание).

Информационные сущности модели Деминга – Шухарта показаны на рис. 9. Видно, что процесс начинается с четкого формулирования целей. Понимание того, какой результат должен быть получен и каким образом он будет оцениваться, есть фундаментальный аспект процесса. В ситуации, когда приемлем любой результат (что получилось, то и ладно), процесс оказывается содержательно разомкнут; все риски приняты заранее и никакого накопления опыта не произойдет.

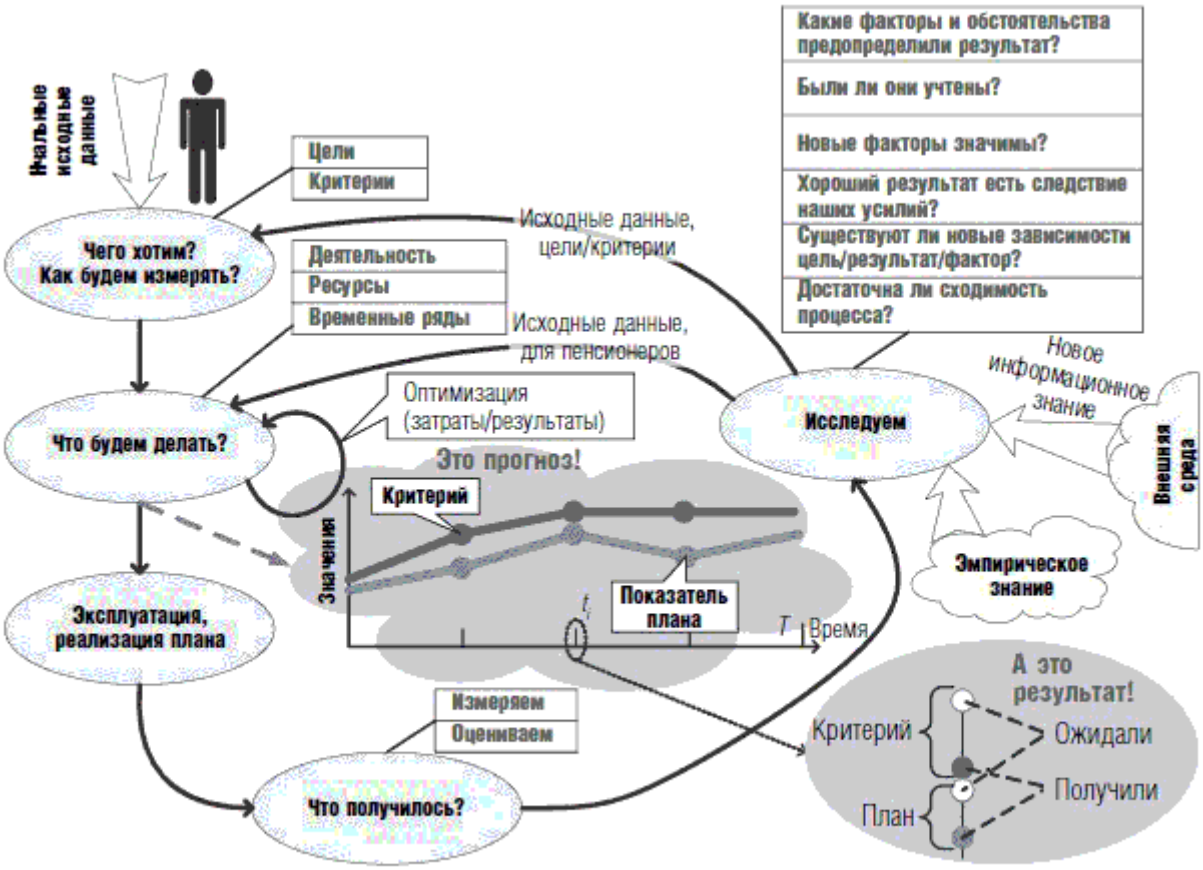


Рис. 9. Информационные сущности модели Деминга — Шухарта

Далее вырабатывается стратегия, отображающая «технологический» аспект: что и как мы будем делать для достижения поставленной цели. В рамках этой стратегии должны учитываться ресурсы и образующийся временной ряд частных (частично реализованных) целей, определяющий количество «проходов» по циклу Деминга (для однократно реализуемой цели). В случае многократной реализации одной и той же цели ситуация упрощается: не требуется детализировать процесс реализации цели. Можно ограничиваться обобщениями по конечным результатам реализации цели. В любом случае на этом этапе составляется план. Далее он реализуется, мы получаем результат и переходим к процедуре его оценки и сравнения с ожидаемым по плану.

И наконец, последним в кольце реализуется аналитический этап. Его задача – понять причину несоответствия реализовавшейся и ожидаемой цели и выработать необходимые корректирующие воздействия. Собственно, на этом этапе и вырабатывается эмпирическое знание в виде некоторой структуры, отображающей причинно-следственные связи и отношения между всеми задействованными в реализации цели субъектами и объектами с учетом условий реализации целей. Для однократно реализуемой цели одной из возможностей является также корректировка собственно самой цели с учетом реализовавшихся частных целей. На рис. 9 эта возможность отражена в виде связи от вершины «Исследуем» к вершине «Чего хотим?».

1.3.10. Интерпретация характеристик риска для управления ИБ

Универсальной моделью измерения уровня ИБ, позволяющей сравнивать результаты оценок ИБ для разных видов целенаправленной деятельности, – модель, основанная на измерении совокупности характеристик риска или риск-факторов.

Будем считать, что оценка уровня ИБ построена на основе некоторой полной модели (модели нулевого риска), описывающей объект некоторой совокупностью реализуемых им

процессов деятельности. Отклонения в реализации процессов будут порождать риски, связанные с их неправильным функционированием (из-за некачественных входных данных или исходного сырья, ошибок персонала, отсутствия должного обеспечения процессов, неправильной поддержки жизненного цикла используемого оборудования и программного обеспечения, злоумышленных действий и т. п.), приводящие в конечном итоге к снижению качества вырабатываемого продукта и другим потерям и негативным последствиям. Оценка ИБ при этом получается двухуровневой:

– характеристики риска каждого процесса, измеряемые по отклонению (отличиям) параметров этого процесса от параметров модели нулевого риска;

– интегральная характеристика совокупного или агрегированного риска, вычисляемая некоторым способом по характеристикам риска отдельных процессов с учетом пересечения множеств факторов.

Эти характеристики риска (т. е. полученные цифровые оценки) ничего не означают до тех пор, пока не накоплено определенное эмпирическое знание о процессах. Идея накопления такого знания в области ИБ состоит в привязывании к этим характеристикам происходящих инцидентов и связанного с ними ущерба. Таким образом, полученная оценка интерпретируется как некий связанный с ней прямой ущерб или негативные последствия, также оцененные по некоторой методике в виде ущерба. Связь оценки с потерями может быть пропорциональной или нет, все зависит от способа агрегирования риска. Описанный процесс интерпретации для случая агрегированного риска иллюстрируется рис. 10.

Обобщенные данные по инцидентам формируются с некоторой периодичностью и оформляются в виде отчетов, содержащих результаты расследования и анализа происшедших инцидентов. Эти результаты, среди прочего, содержат суммарную величину ущерба за отчетный период, полученного от инцидентов. Сопоставляя эту величину с интегральной оценкой, характеризующей риск и вычисленной в начале отчетного периода, можно получить множество точек в координатах «ущерб, риск», по которым может быть построена соответствующая зависимость. С использованием полученной зависимости возможно выполнить прогноз ущерба для следующего интервала отчетности. Риск принимается, если прогнозируемый ущерб будет меньше допустимого значения. В противном случае риск должен обрабатываться.

Предполагается, что интервалы отчетности одинаковы по величине. При необходимости прогноза ущерба на более короткий или более длинный интервал по сравнению с интервалом отчетности зависимость должна соответствующим образом трансформироваться. Если говорить о тенденциях, то при более длинных интервалах ущерб при одной и той же интегральной оценке риска будет возрастать, а при более коротких интервалах сокращаться (см. графики на рис. 10 справа).

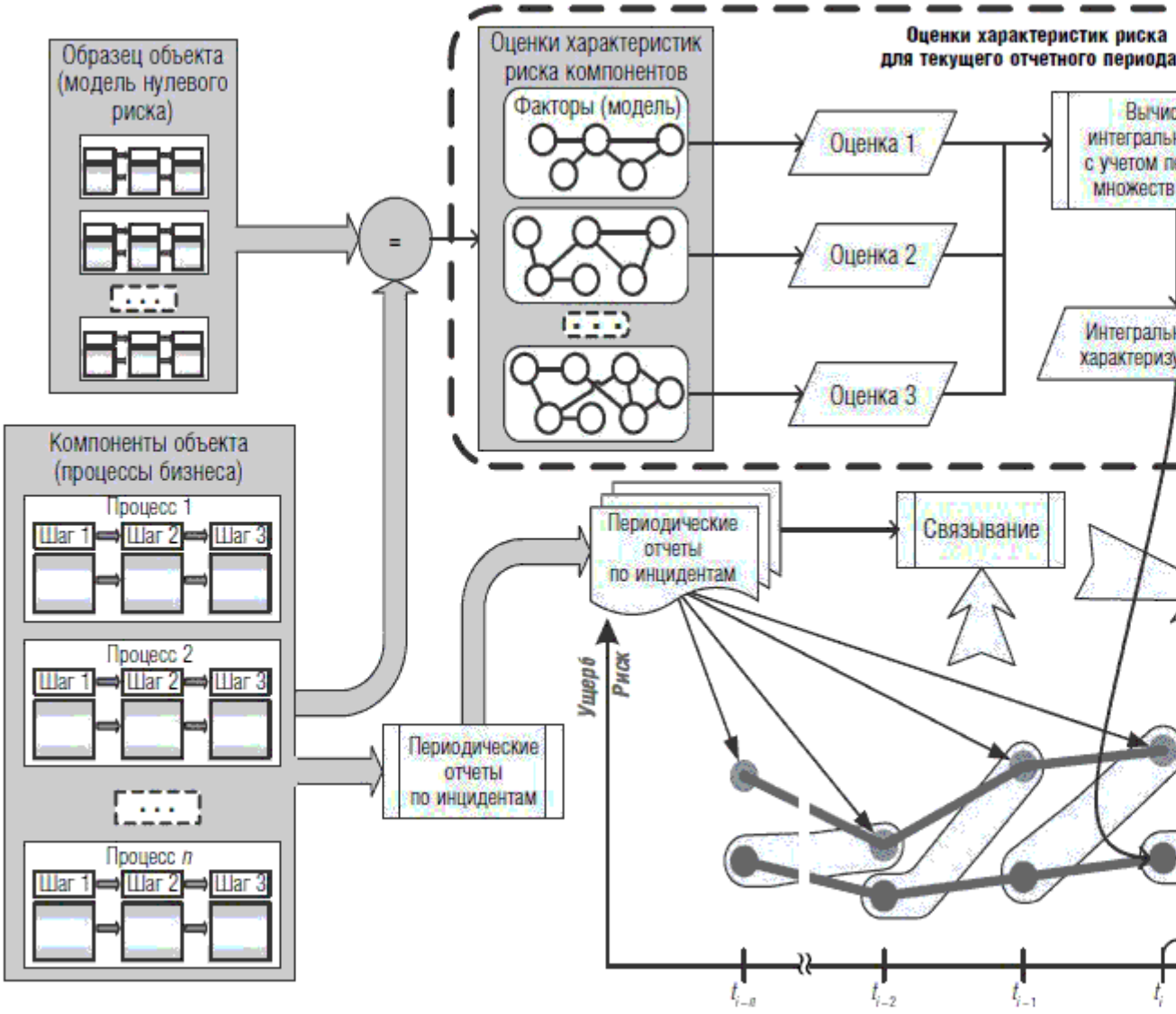


Рис. 10. Интерпретация интегральной оценки, характеризующей совокупный

Обработка риска предполагает воздействие на объект, в результате которого должна происходить некоторая его реструктуризация. Сила этого воздействия может быть измерена величиной инвестиций, необходимых для реструктуризации и улучшения функционирования процессов, приводящих в конечном счете к уменьшению ущерба. При этом можно использовать разные стратегии: инвестировать понемногу во все процессы или выбрать для инвестирования какую-то группу процессов. Один из подходов, иллюстрация которого приведена на рис. 11, предполагает накопление ряда значений оценок ущерба для каждого из процессов с учетом инвестиций. В результате может быть построена зависимость, характеризующая чувствительность процесса к инвестициям. Разные процессы могут находиться в разном состоянии и поэтому иметь разную чувствительность к инвестициям. Одни процессы имеют линейную зависимость (см. рис. 11, верхний график), другие требуют для получения нужного эффекта больших начальных вложений (нижний график), третьи процессы близки к насыщению, и слишком большие инвестиции в них не дадут нужного эффекта (средний график на рис. 11).

Например, установка сетевого экрана с функциями обнаружения вторжений в условиях, когда его не было и для защиты компьютеров во внутренней сети использовались средства, штатно имеющиеся в составе их ОС, потребует сразу больших инвестиций. Когда же этот экран установлен и необходима лишь корректировка правил фильтрации и настройка системы обнаружения вторжений, то вложения будут относительно небольшими, причем

эффект от этого мероприятия будет ограничен теми возможностями по настройке, которые есть в имеющемся оборудовании. Затраты на сверхтонкую настройку при ограниченности возможностей, как правило, не оправдывают себя.

Размер инвестиций определяется величиной прогнозируемого ущерба, поскольку если на преодоление риска требуется ресурс больший, чем потери, то нет смысла обрабатывать риск. В приводимом на рис. 11 примере размер инвестиций таков, что в нижний процесс на рисунке его не имеет смысла вкладывать. Второй процесс имеет смысл инвестировать в небольшом объеме. Оставшуюся часть целесообразно инвестировать в первый процесс.

В рассмотренных иллюстрациях цикл накопления знаний вырождается в совершенствование обработки риска. Отметим, что построение использованных в примерах зависимостей по эмпирическому опыту чаще всего окажется невозможным. Назначение рассмотренных примеров – облегчить понимание природы связи абстрактных оценок риска с имеющейся практикой. Это понимание облегчит и позволит совершенствовать обработку риска даже в том случае, когда она делается на основе экспертных оценок.

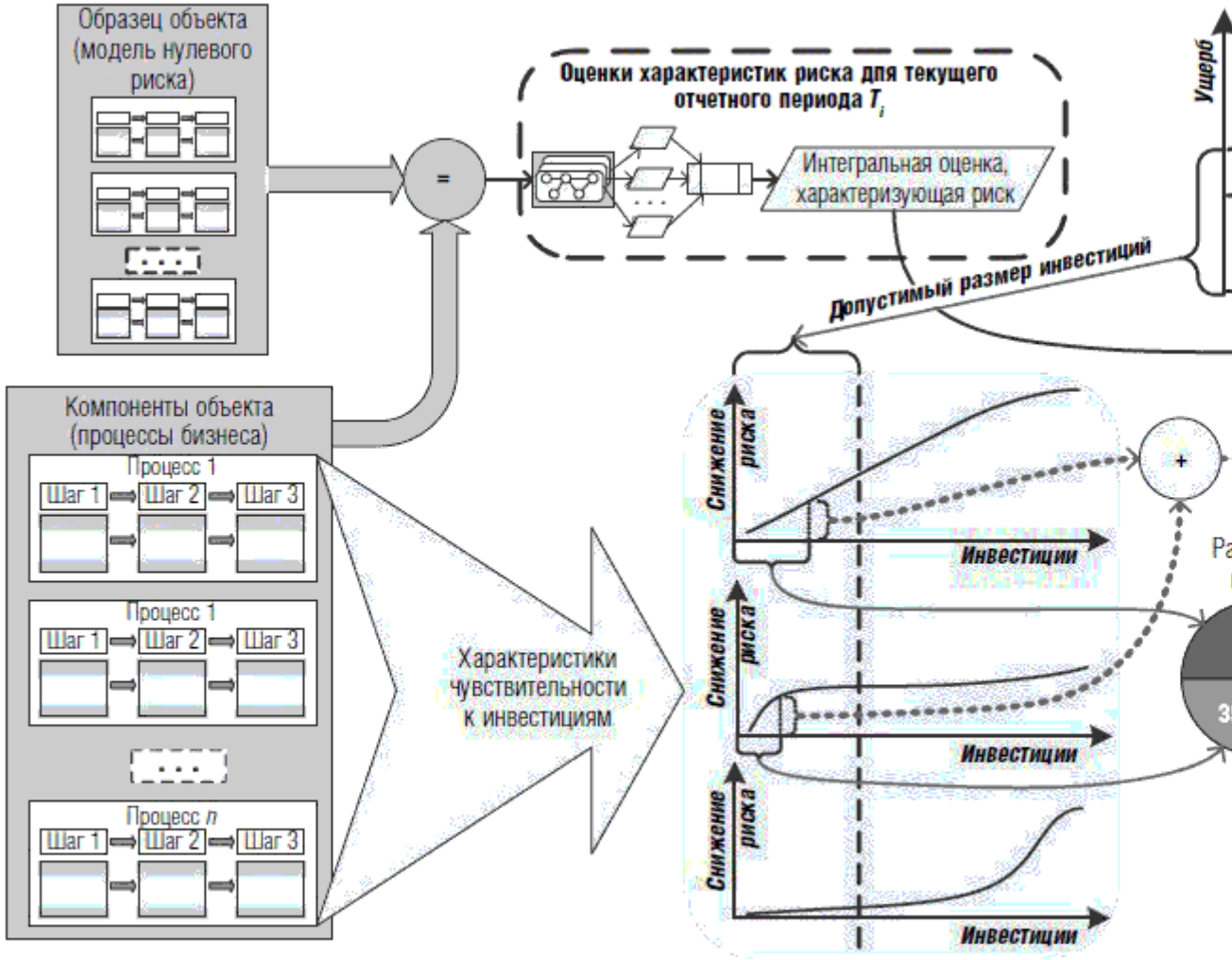


Рис. 11. Обработка риска с учетом распределения инвестиций

1.3.11. Общая модель обеспечения ИБ бизнеса

Теперь можно сформулировать основные требования к архитектуре (структуре) модели. Понятно, что ее ядром должны стать процедуры и механизмы накопления и обобщения знаний, и прежде всего эмпирических. Предметная область (о чем знания) – факторы и обстоятельства, препятствующие и способствующие достижению поставленных

целей, отображенные в информационную сферу (все, что существует и используется в виде описаний). Необходимая направленность (применимость) знаний – эффективное противодействие рискам в информационной сфере независимо от их природы.

Риск рассматривается как сущность, определяемая в пространстве факторов «А, П, И, С, Р». Он же (риск) является сущностью, посредством которой осуществляется отображение ИБ на базовые риски бизнеса и далее на его потенциальные ущербы и негативные последствия. С учетом этих соображений общая модель обеспечения ИБ бизнеса представлена на рис. 12.

Эта модель представляет собой одну из разновидностей модели Деминга – Шухарта, а именно модель с центральным фокусом. В фокусе модели размещаются аналитический функционал и база лучших практик, обеспечивающие накопление и обобщение знаний, а также настройку параметров функций и процессов, размещенных непосредственно в кольце, и управление ими (прежде всего запуском).

Видно, что процесс идентификации факторов влияния на заданные цели, являющийся стартом кольца, реализуется непрерывно и отражает потребность в выявлении новых факторов и обстоятельств, способных повлиять на цели деятельности. Для этого фокус использует любую доступную для него информацию, как внутреннюю, так и внешнюю. Любые зафиксированные изменения (изменчивость) приводят к запуску процессов оценки (вершина «Оценка» на рис. 12), второе условие запуска – «по интервалу времени» принудительно. Измеряются допустимые значения идентифицированных рисков ИБ. Если изменения значимы, как показано на рис. 12, то запускаются процессы обработки рисков (вершина «Обработка»), в противном случае кольцо замыкается.

Процессы обработки рисков в качестве результата вырабатывают комплекс мер реагирования на изменившееся распределение рисков ИБ с учетом накопленного знания. Далее процессы оптимизации (вершина «Оптимизация» на рис. 12) интегрируют новые меры реагирования в систему уже имеющихся с учетом ограничений на ресурсы и величины принимаемого риска для целей деятельности. При этом каждый раз рассматривается вся действующая система мер реагирования в контексте «цель; принятый риск; ресурс» и вырабатывается наилучшая в смысле накопленного знания система мер. Далее осуществляется ее экспорт в пространство «А, П, И, С, Р», на чем процесс улучшений завершается, а кольцо Деминга замыкается по полному циклу.

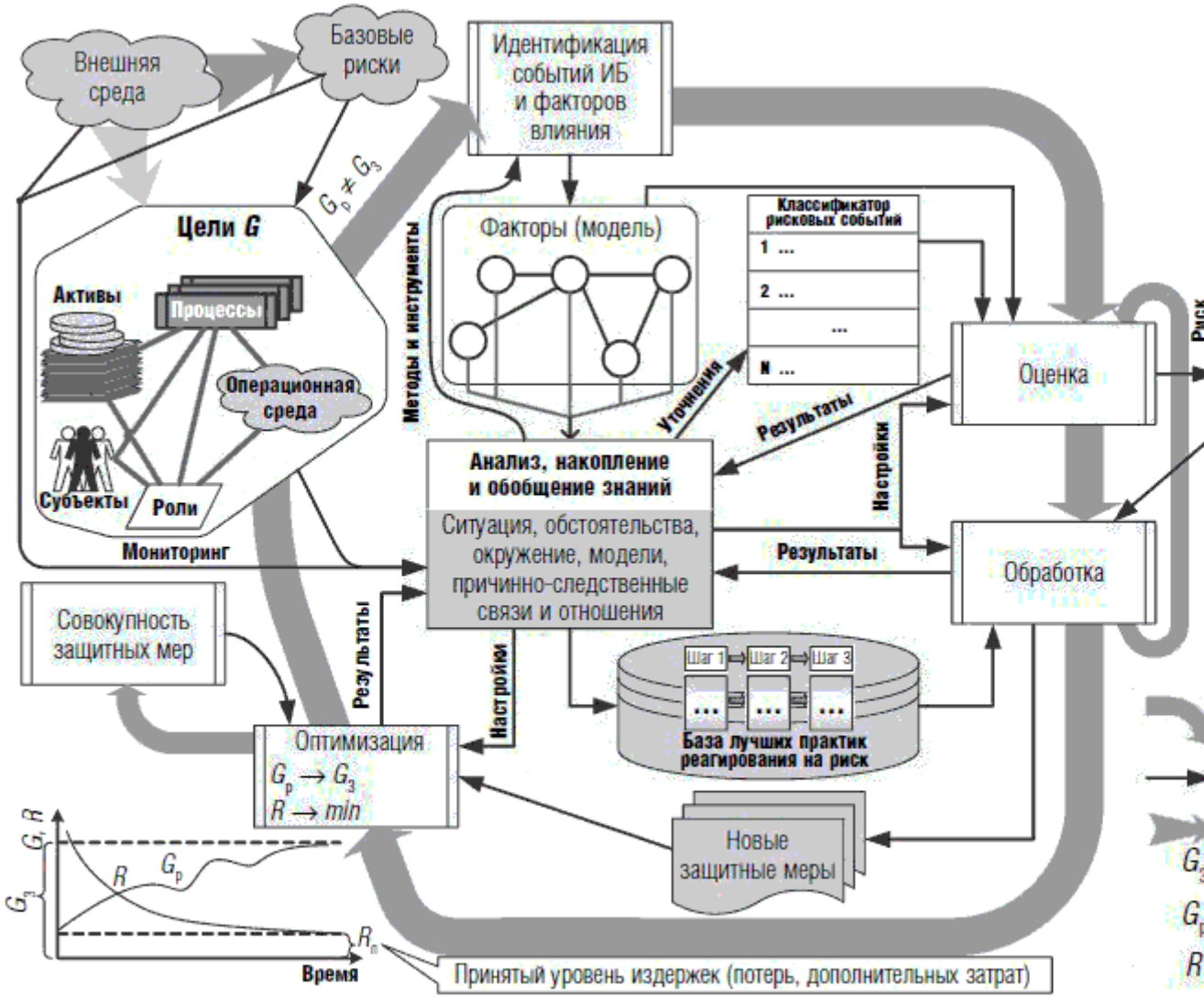


Рис. 12. Общая модель обеспечения ИБ бизнеса. Основные сущности и взаимосвязи

Видно, что приведенная на рис. 12 общая модель обеспечения ИБ организации есть некоторая рациональная композиция процедур, механизмов и методов, рассмотренных выше, почему и нет необходимости подробно ее описывать. Это в известном смысле «идеальная» модель обеспечения ИБ организации. Реальные потребности организации могут ее изменять, усиливая одни компоненты и ослабляя либо исключая другие компоненты. Однако основная проблема практической реализации модели состоит не в этом, а в сложности ее интеграции в сложившийся в организации набор практик менеджмента различными аспектами ее деятельности.

1.3.12. Проблемы практической реализации модели обеспечения ИБ организации

Любая организация в процессе своей деятельности накапливает набор практик, обеспечивающих реализацию тех или иных ее потребностей. В совокупности они составляют сбалансированную естественным образом самой организацией систему менеджментов. Как правило, это уникальная система, отражающая конкретную практику конкретной организации. В том числе, если речь не идет об организации, создаваемой заново, в этой практике есть и уже сложившаяся система обеспечения ИБ, также уникальная. В этой связи успех или неуспех практической реализации рассмотренной модели ИБ в организации будет определяться тем, насколько она «гармонизирована» со сложившейся практикой. Основные,

сильно влияющие на проблему гармонизации аспекты следующие:

– модели, реализуемые в рамках общекорпоративного менеджмента;

– модели внутреннего контроля и аудита организации;

– модели кадрового менеджмента;

– модели совершенствования и управления ИТ-системами организации;

– модели, используемые в бизнес-аналитике организации;

– модели общего риск-менеджмента организации;

– внутренняя нормативная база, определяющая роли и организационные политики организации, а также вопросы владения активами организации;

– стратегический и оперативный уровни управления организацией. Приведенный перечень только основных аспектов влияния на обеспечение ИБ в организации показывает сложность проблемы гармонизации. Очевидно, что ее решение существенно упростится, если методологические основы (платформы) близки или вообще совпадают. Это, однако, не так. Например, часть реально применяемых моделей рассматривают формализуемые ими сущности (объекты, процессы, технологии, виды деятельности и т. д.) как самодостаточные и не учитывают при этом фундаментальный аспект эффективности деятельности; не предполагают сопоставление получаемого результата (эффекта) и потребностей в инвестициях. К подобным моделям относится, например, ISO 9000, подвергаемый суровой критике за эту свою особенность.

Общекорпоративный менеджмент во многих организациях методологически основан на реагировании на возможные проблемы, а не на их избежании. Риск-менеджмент не везде хорошо развит, вследствие чего важнейшая функция процесса целенаправленной деятельности по идентификации и анализу причинно-следственных связей между происходящими событиями и понесенными ущербами не реализуется. Преодоление этих и многочисленных других противоречий усилиями только одной безопасности невозможно.

Однако не только эти особенности организации влияют на реализацию модели обеспечения ИБ. Некоторые специфические свойства проблемы обеспечения ИБ, отображаясь на систему менеджментов организации, могут приводить к появлению различных «вырожденных» случаев как в части модели Деминга – Шухарта, так и в части информационно-аналитической и оценочной деятельности в рамках модели обеспечения ИБ организации. Рассмотрим основные из них.

Во-первых, это проблема реализации изменчивости системы обеспечения ИБ организации. Суть проблемы реализации изменчивости заключается в объективной существующей консервативности систем обеспечения ИБ, изменчивость которой осуществляется фактически по «жизненным показаниям». В то же время модель Деминга – Шухарта, являющаяся основой приведенной выше (см. рис. 12) общей модели обеспечения ИБ бизнеса, наиболее полезна в условиях изменчивости. В общем случае чем короче будет цикл выполнения процессов модели Деминга – Шухарта, тем больший эффект будет получен.

Природа консервативности систем обеспечения ИБ состоит в том, что на практике безопасность всегда следует за бизнесом (целями деятельности) и вынуждена, по крайней мере на первых порах, обходиться тем, что уже есть, что уже реализовано и опробовано, так как инвестиционный процесс даже в очень продвинутой организации создаст неоправданно большую задержку. Реально от момента осознания руководством потребности до ввода нового компонента безопасности в промышленную эксплуатацию может проходить 1–3 и даже более лет. В течение этого интервала реализуются временные меры обеспечения ИБ, и если реально сложившийся уровень риска будет принят высшим руководством, то инвестиционный процесс вообще не будет запущен.

На практике изменчивость системы обеспечения ИБ обусловлена факторами, связанными с реализацией трех процессов:

– вывода компонентов системы, цели деятельности которых (предназначение) исчерпаны, из эксплуатации;

– модернизации компонентов системы;
– интеграции в систему обеспечения ИБ новых компонентов.

Необходимость модернизации или замены старого оборудования на улучшенное новое диктуется двумя причинами:
– проблемами поддержки жизненного цикла (например, из-за прекращения поддержки каких-то продуктов);
– необходимостью компенсировать дополнительные риски, идентифицированные при модернизации бизнес-процессов или возникшие вследствие другой изменчивости.

Потребность в интеграции новых компонентов возникает, как правило, в связи с изменениями законодательной и иной нормативной базы, запуском нового вида бизнеса, потребности в безопасности которого не удалось обеспечить уже имеющимися средствами, а также вследствие существенной изменчивости любого другого вида.

Перечисленные три процесса одномоментно охватывают незначительную часть системы безопасности (ориентировочно 5–7 %) и находятся в разных фазах реализации. К тому же они в зависимости от потребностей перемещаются со временем по системе («плавают»). Проблема управления этими процессами в модели обеспечения ИБ (см. рис. 12) в основном отнесена к блоку «Оптимизация».

Очевидно, что для целей управления этими процессами должна существовать система оценки, обеспечивающая принятие адекватных решений. Теоретически она может быть достаточно хорошо формализована, но практически в этом нет потребности. Гораздо полезнее на практике оказывается наличие хорошо разработанного документа по стратегическим улучшениям ИБ в организации, содержащего четко сформулированные цели, которые нужно достичь, и систему критериев (приоритетов), которыми нужно руководствоваться при принятии адекватных решений.

Важнейшими из них должны быть критерии, обеспечивающие организационную, техническую и технологическую целостность системы безопасности в условиях изменчивости. Можно привести много примеров того, когда простое изъятие уже отработавшего свое компонента в системе приводило к нарушению ее целостности, так как изымаемый компонент создавал дополнительный функционал для других компонентов и это не было учтено.

Вообще, проблема обеспечения целостности системы обеспечения ИБ важна и актуальна сама по себе. Дело в том, что безопасность – единственный вид деятельности в организации, которым в той или иной мере должны заниматься все. Это ее свойство. Одновременно это создает высшему руководству иллюзии о возможности ее полной децентрализации, тем более что частично децентрализации всегда есть, особенно в части поддержки владения активами (ресурсами). Однако чем более децентрализуется система, тем больше утрачивается ответственность за конечный результат и тем больше вероятность образования в системе разрывов, создающих риски. Практика показывает, что наличие единого и сильного (в смысле прав и обязанностей, ответственности) центра управления является жизненно необходимым как с точки зрения достижимости требуемого результата, так и обеспечения эффективности деятельности.

Другой важнейшей для практики особенностью модели обеспечения ИБ организации является то, что фактически она реагирует на возникающую изменчивость внутри и вне организации и автоматически локализуется на выявленной изменчивости. Нет никакой практической необходимости в тотальной реализации всех ее процессов применительно ко всей системе на постоянной основе. Действительно, вновь идентифицированный риск требует детального анализа и оценивания, равно как и иных, предусмотренных моделью процедур. Однако в дальнейшем значимым факторов является уже не сам риск (он уже обработан), а то, что с ним происходит: он растет; остается неизменным; убывает.

В этой связи существенно упрощаются оценочные процедуры – от оценки рисков

можно перейти к риск-ориентированным оценкам, рассмотренным подробно в следующих главах. Кроме того, после идентификации новых рисков можно перейти к оценочным технологиям, основывающимся на оценках параметров реально произошедших рисковых событий. Примером таких технологий является оценка по методу VAR (value at risk, первоисточник с описанием метода в [1]), т. е. оценка величины понесенных потерь за некоторый фиксированный интервал времени. Этот метод в силу его простоты и наглядности имеет очень большое распространение.

Широко используются также оценочные системы, основанные на измерениях различных функциональных параметров, прямо или косвенно характеризующих значимые для безопасности состояния объектов и систем. Эти показатели называют ключевыми индикаторами риска (КИР). Превышение порогов по КИР либо возникновение нежелательных трендов инициирует уже более детальный анализ и оценивание причин этих явлений. Одним из КИР может служить, например, количество зафиксированных нарушений персоналом регламентов обработки значимых активов за один день по всей организации.

Таким образом, говоря о практической реализации модели ИБ, организации нужно иметь в виду следующее:

– она локализуется в области возникновения и распространения изменчивости;

– ее процессы реализуются каждый раз с разной степенью детализации в зависимости от возникающей потребности;

– для достижения желаемого результата может использоваться широкий спектр оценок, характеризующих риск;

– заложенная в модели цикличность не является постоянной ни по структуре цикла, ни по времени его реализации, она существенно зависит от реализовавшихся условий запуска и параметров внешних по отношению к модели процессов организации, например того же инвестиционного процесса;

– одномоментно в стадии реализации в зависимости от сложившейся ситуации может быть несколько еще не завершенных циклов, находящихся на разных фазах реагирования на инициировавшие эти циклы проблемы; наиболее значимая из них будет автоматически (в соответствии с оценкой) получать приоритет по использованию общих ресурсов и процедур.

Главный практический результат реализации модели обеспечения ИБ в организации состоит в том, что деятельность безопасности получает качественную объективную основу, становится существенно более прозрачной и предсказуемой для высшего руководства и бизнеса организации как по ее потребностям (инвестициям в безопасность), так и по ожидаемым результатам. Она создает условия для «естественной» интеграции безопасности в систему общекорпоративных менеджментов и бизнес.

2. Существующие модели менеджмента (управления), применимые для обеспечения информационной безопасности бизнеса

Если организация располагает неограниченным ресурсом, то проблемы управления для обеспечения информационной безопасности ее бизнеса не существует. Если это не так и ресурс имеет ограничения, то тогда проблемы управления актуальны.

2.1. Модели непрерывного совершенствования

2.1.1. Модели непрерывного совершенствования и корпоративное управление

Наряду с тезисом, вынесенным в преамбулу раздела, представляется необходимым

сформулировать еще ряд тезисов, имеющих прямое и /или косвенное отношение к вопросам управления (даже не только и не столько управления, сколько обеспечения) информационной безопасности организации, как в целях улучшения (совершенствования), так и для целей поддержания (сохранения) безопасности на заданном уровне:

– в теории нет разницы между теорией и практикой, а на практике есть;

– безопасность и сложность несовместимы;

– безопасность всегда имеет тенденцию к ослаблению;

– любое изменение, вносимое в систему (операционную среду организации), в первую очередь ослабляет ее безопасность.

Обсуждая в формате книжного издания такую многогранную проблему, как управление (менеджмент), невозможно не затронуть вопросы теории, в то же время практика всегда дает «настройку» любой теории и в итоге прямо или косвенно выносит ей свой вердикт. Теория – это, как правило, продукт научных исследований и изысканий, в том числе и продукт анализа и синтеза наблюдаемых явлений; ее жизнеспособность должна опять же подтвердить практика (натурный эксперимент, опытная партия и т. п.). Далее будут рассмотрены вопросы теории и практические аспекты задачи менеджмента (управления), применимые для обеспечения информационной безопасности бизнеса.

Информация о наличии организационных структур в практике управления (менеджмента) обнаружена еще на глиняных табличках, датированных III тыс. до н. э. Однако, хотя само управление достаточно старо, идея управления как научной дисциплины, профессии, области исследований относительно нова. В наши дни в сфере управления организационно-техническими системами накоплен богатейший опыт, позволивший в начале XX в. определить управление как целостное направлении науки и техники, имеющее свои ветви и течения, приверженцев и оппонентов. Преимущественно началом XX в. датируется наибольшее число ветвей науки управления, получивших широкое распространение в наши дни. Одной из первых работ можно отметить «Принцип научного менеджмента» [2], опубликованный в 1911 г. Фредериком Тейлором, традиционно считающийся началом признания управления наукой и самостоятельной областью исследований. Понятия о систематизированном управлении организацией стали формироваться в середине XIX в. Успехи в теории управления всегда зависели от успехов в других, связанных с управлением областях, таких как инженерные науки, психология, социология, математика и др. По мере развития этих областей знаний теоретики и практики управления узнавали все больше о факторах, влияющих на успех организации. Руководители организаций, предприниматели, ученые стали глубже осознавать влияние внешних по отношению к организации сил и условий. Специальные исследования позволили разработать новые подходы в управлении.

Существенное влияние на используемые модели управления оказывали факторы экономической и социальной среды организаций, общественный строй и др. Перемены 1990-х гг. привели к востребованности в российской практике международного опыта, включающего принципы, модели, стандарты и практики управления, адаптированного к национальным условиям.

В то же время многое, имеющее отношение к управлению, определяется целями и задачами, решению которых должна отвечать система управления (объекта, деятельности, организации и т. п.).

Любая организация создается и функционирует для реализации каких-либо задач. Даже если взять абстрактный случай, когда организация создается не для достижения ею каких-либо целей, а для того, чтобы она номинально существовала, то для целей самосохранения компания обязана поддерживать некоторые виды деятельности (процессы) и иметь соответствующую систему управления.

Обобщенная модель корпоративного управления приведена на рис. 13. Корпоративное управление в общем случае имеет два уровня: «управление должностных лиц через совет директоров, выбираемый акционерами» и «управление деятельностью (бизнес-процессами/деловыми операциями), осуществляемое должностными лицами». Это

верхний уровень управления, который следует иметь в виду всякий раз, когда идет речь о высшем руководстве организации, принимающем значимые решения в сфере менеджмента информационной безопасности бизнеса.

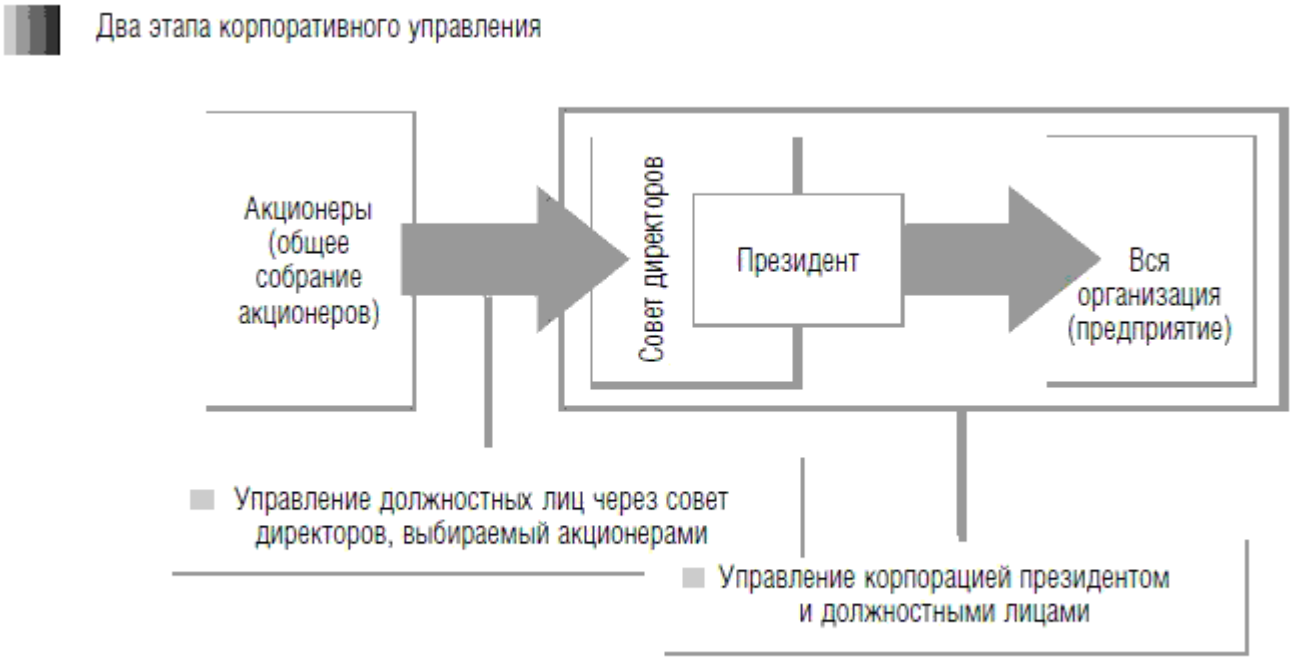


Рис. 13. Корпоративное управление

Если должностные лица не управляют корпорацией, управление должностных лиц через совет директоров, выбираемый акционерами, ничего не значит и никакие ожидания собственников (акционеров) не будут иметь под собой твердых оснований. Поэтому управление бизнес-процессами должностными лицами так называемого уровня правления (исполнительского уровня) имеет первостепенное значение. Это управление требует осуществления так называемого менеджмента.

Понятие «менеджмент» является для России заимствованным (американское определение менеджмента – «делать что-либо руками других» [3]). Несмотря на то что в последние десятилетия оно получило достаточно широкое распространение как в сфере экономики и финансов, так и в производственной деятельности, в среде специалистов по защите информации, структур, регулирующих вопросы технической защиты информации, чаще всего используются понятие «управление», нежели «менеджмент». В гармонизируемых в России в последнее десятилетие международных стандартах по информатизации и информационной безопасности англоязычное понятие management переводится и как «управление», и как «администрирование». В то же время понятия «менеджмент» и «управление» имеют свои, давно сформировавшиеся определения, данные в гармонизированных в России международных стандартах качества серии ГОСТ Р ИСО 9000, а также базовых модельных стандартах менеджмента риска и безопасности, таких как ГОСТ Р 51897 [4] и ГОСТ Р 51898 [5], отражающих гармонизированные (адаптированные) международные модельные руководства.

Так в стандартах ГОСТ Р ИСО 9000 понятие менеджмент определено как «*скоординированная деятельность по руководству и управлению организацией».* При этом поясняется, что «в *английском языке термин "management" иногда относится к людям, т. е. к лицу или группе работников, наделенных полномочиями и ответственностью для руководства и управления организацией. Когда "management" используется в этом смысле, его следует всегда применять с определяющими словами с целью избежания путаницы с понятием "management", определенным выше. Например, не одобряется выражение "руководство должно…", в то время как "высшее руководство должно…" – приемлемо».*

Для определенных практических целей представляется возможным использование как

понятия «менеджмент», так и «управление» – как наиболее привычного для российских специалистов, четко определяя при этом то, что мы понимаем под этими понятиями в каждом конкретном случае.

По аналогии с неуправленческими видами деятельности предпринимались попытки выделить в процессе менеджмента определенные функции – концептуальные элементы в содержании работы руководителя. Результатом явилась функциональная модель управления, перекликающаяся с определенными Анри Файолем в 1916 г. административными операциями (предвидение, организация, распорядительство, координирование и контроль). Данная модель представляет процесс управления в виде замкнутого цикла: планирование – организация – мотивация (лидерство) – контроль.

Безусловно, функциональная модель представляет собой скорее абстракцию; как показали исследования Генри Минцберга, практическая сторона работы менеджера в значительной мере неструктурированна, дискретна и спонтанна. Минцберг выявил четыре общепринятых мифа (заблуждения) относительно содержания управленческого труда.

Миф № 1: работа менеджера (в российской практике – управленца того или иного звена и уровня) состоит в систематическом и сознательном планировании. Примеров такой позиции множество. Но ни один из исследователей не приводит достаточных свидетельств в ее пользу.

Факты. Целый ряд исследований показывает, что менеджерам приходится работать в чрезвычайно высоком темпе. Основные черты процесса управленческого труда – краткость, разнообразие и непрерывность. Менеджеры ориентированы прежде всего на действие.

Миф № 2: у хорошего менеджера нет никаких текущих обязанностей. Говорят, что менеджеры все время заняты разработкой грандиозных планов и распоряжениями, а все текущую работу поручают другим – не дело менеджера заниматься мелочами. Если воспользоваться распространенным сравнением, то можно сказать, что хороший менеджер, как и хороший дирижер, все отшлифовывает заранее, а затем сидит и наслаждается результатами своего труда, лишь реагируя на те или иные непредвиденные обстоятельства.

Факты. Менеджер действительно несет ответственность за принятие решений в непредвиденных обстоятельствах, но, помимо этого, он имеет массу текущих обязанностей, включая исполнение разного рода обязанностей, участие в переговорах, анализ и обработку информации, связывающей организацию с окружающим миром.

Миф № 3: для старших менеджеров требуется уже обработанная информация. С такой задачей лучше всего справляются формальные информационные подразделения. Согласно такому мнению, менеджер должен находиться на самой вершине иерархической системы информации. Такой менеджер «по переписке» вообще должен всю важную информацию получать от гигантских, всезнающих управленческих информационных систем.

Факты. На самом деле все обстоит иначе. У каждого менеджера есть свои собственные средства получения информации и данных: документы, телефон, запланированные встречи и встречи вне расписания, ознакомительные поездки. Иными словами, менеджеры активно пользуются вербальными средствами – телефоном и личными встречами.

Миф № 4 практический менеджмент – это профессия и наука (или вскоре станет таковой).

Факты. Если сопоставить это мнение с любыми определениями науки, оно явно неверно. Реальная работа менеджера далека от научных исследований. Наука включает в себя систематические, аналитически продуманные программы и процедуры. Но если мы даже толком не знаем, какие именно процедуры выполняет менеджер, как можно требовать от них научной аналитичности. Таким образом, все менеджерские программы: расписание, информационный процесс, принятие решений и т. д. – находятся в его голове. А потому, чтобы как-то описать эти программы, нам приходится полагаться на слова, суждения и интуицию. И очень редко мы отдаем себе отчет, что все это – не более чем знак нашего неведения.

Однако вернемся к вопросу моделей управления. Собственникам (см. рис. 13,

акционеры, общее собрание акционеров) и их полномочному органу – совету директоров необходимы инструменты взаимодействия с исполнительными органами, обеспечивающие уверенность их в том, что принятые ими решения будут исполнены, ожидания от результатов деятельности организации будут иметь основания и т. п. В идеале любой собственник (как частный, так и государственный) желает так «настроить» деятельность организации, чтобы, единожды запустив ее работу, более не вмешиваться, а получать лишь дивиденды. Для удовлетворения подобных ожиданий модели и принципы управления организации должны подразумевать возможность (давать основу) реализации условий самосовершенствования, самоадаптации организации к изменениям ее среды, как внешней, так и внутренней.

Указанным потребностям в полной мере удовлетворяет упоминавшаяся ранее в предыдущем разделе модель (цикл) Деминга – Шухарта. Она легла в основу большинства современных управленческих стандартов для различных областей деятельности и «де-факто» становится базовой моделью. Как отмечается в книге Г. Нива «Пространство доктора Деминга» [6], «“Цикл Деминга” известен еще и как “Цикл Шухарта”, цикл “PDCA” или цикл “PDSA”». Деминг ссылается на него как на «Цикл Шухарта», поскольку его идея, по-видимому, имеет своим источником книгу Шухарта 1939 г. В то же время в практике обычно на него ссылаются как на «Цикл Деминга». Аббревиатура же циклов «PDCA» и «PDSA» раскрывается как «планируй – сделай – проверь – действуй» для PDCA и «планируй – сделай – изучи – действуй» для PDSA. Аббревиатура PDCA является наиболее распространенной, хотя сам Деминг более предпочитает использовать PDSA».

Книга Шухарта, как отмечает Г. Нив, начинается с выделения трех стадий в управлении качеством результатов деятельности организации:

– разработка «Спецификации» (техническое задание, технические условия, пределы и пороги, критерии достижения целей) того, что требуется;

– производство «Продукции», удовлетворяющей «Спецификации»;

– проверка («Контроль») произведенной «Продукции» для оценки ее соответствия «Спецификации».

Шухарт одним из первых предложил линейное восприятие указанных стадий замкнуть в цикл, который он отождествил с «динамическим процессом приобретения знаний». После первого цикла результаты «Контроля» должны являться основой *совершенствования* «Спецификации» на продукцию. Далее производственный процесс корректируется на основе уточненной «Спецификации», а новый результат производственного процесса опять же подвергается «Контролю» и т. д.

Три стадии цикла Шухарта: «Спецификация – производство Продукции – Контроль» – во многом подобны задачам первых трех стадий в циклах PDCA или PDSA Деминга. Как отмечает Г. Нив [см. 6], версия цикла Деминга, рассмотренная в его работе «Выход из кризиса» [7], хотя и имеет четыре стадии, но на самом деле ее третья и четвертая стадии («проверь» или «изучи» и «действуй») – это скорее результат разделения третьей стадии «контроль» модели Шухарта на две новые, более четко выделенные стадии, которые можно охарактеризовать как «наблюдение» и «анализ». Как и в случае с «циклом Шухарта», «цикл Деминга» представлен в виде, который позволяет понять, что последовательность шагов должна повторяться на качественно новом уровне, используя знания, накопленные на предшествующем цикле.

Здесь уместен достаточно наглядный пример практической реализации модели Деминга PDCA, имеющийся в книге Г. Нива [см. 6] и иллюстрирующий «работу» одной из стадий модели. Компания Nissan неожиданно для участников рынка начала скупать бывшие в употреблении малолитражные машины, включая разбитые, и отправлять их в Японию. Количество машин, приобретаемых компанией Nissan, измерялось в тысячах. Четырьмя годами позже вышла модель автомобиля Nissan Micra, которая была признанной одной из лучших в своем классе. Так вот, отгрузка в Японию подержанных и разбитых

малолитражных машин было частью стадии (процесса) планирования для автомобиля Nissan Micra.

Уместен и еще один пример последних лет: когда организация принимает иную стратегию действий в связи с условиями на рынке (рынок достаточно насыщен, организация – новый участник рынка, необходимо оперативно занять свою нишу). Данная стратегия диаметрально противоположна рассмотренной стратегии компании Nissan и концентрирует усилия организации не на планировании, а на контроле – максимально оперативной реакции организации на мнение рынка и отзывы потребителей. В рамках освоения российского рынка один китайский автопроизводитель поставили группе московских дилеров первую партию из 200 автомобилей, абсолютно новых для нашего рынка. Продукция имела массу недостатков, как конструктивного, так и эстетического плана, и не выдерживала никакой критики (даже в соотношении цена/качество). Получив отзывы на первую партию, компания-производитель через три месяца направила следующую партию, в продукции которой около 80 % замечаний и недостатков были устранены, включая и те, что затрагивали техпроцесс изготовления изделия и изменения конструкции. Результат не заставил себя ждать – товар стал находить своего потребителя.

И в первом, и во втором примере мы видим работу моделей управления компанией, отвечающих модели (циклу) Деминга – Шухарта.

Модель Деминга фактически приводит нас к мысли о необходимости не только регулярного контроля, но и использования знаний, накопленных на предшествующих этапах модели или полных циклах, в совершенствовании своей деятельности. Используя подобную модель и рассматривая процессы (виды деятельности организации), управляемые согласно им во временной ретроспективе, мы получаем возможность спрогнозировать будущие результаты этих процессов. В связи с этим существуют интересные оценки возможностей системы управления (менеджмента) организации. Не более 15 % всех проблем (или возможностей улучшения) в организациях связано с возможной вариацией в реализации производственных процессов, которые могут быть в поле зрения рядовых работников. Тогда как на долю менеджеров приходится как минимум 85 % от всех потенциальных возможностей улучшений системы, в которой работают их служащие. После проверки этих чисел на протяжении многих лет д-р Деминг пересмотрел их и в 1985 г. дал новую оценку, соответственно 6 и 94 % [6].

Модель Деминга – Шухарта получила широкое применение не только в стандартах качества ГОСТ Р ИСО 9000 и экологии ГОСТ Р ИСО 14000, но и в стандартах иных видов деятельности организаций – не только отраслевых, таких как автомобилестроение и цепочки поставок и безопасность продуктов питания, но таких специфичных, как информатизация и безопасность. Везде, где объектом рассмотрения может быть деятельность и применим процессный подход, развивается и внедряется модель менеджмента, основывающаяся на циклической модели Деминга – Шухарта.

Со временем модель Деминга – Шухарта получила свое практическое применение на всех уровнях деятельности организации, связанной с безопасностью, и на всех направлениях обеспечения безопасности (экономической, информационной, физической и пр.). Фактически это является отражением того, что любая деятельность независимо от области применения должна изначально (по возможности тщательно) планироваться, а ее реализация наряду с поддержкой – контролироваться (проверяться) и при необходимости совершенствоваться, обеспечивая адаптацию к изменениям как в среде рассматриваемой системы, так и в ней самой.

2.1.2. Вопросы реализации моделей непрерывного совершенствования и процессного подхода в организации

В практической деятельности при работе над внедрением в различных организациях систем менеджмента информационной безопасности, систем менеджмента

информационными активами организации, систем менеджмента рисками информационной безопасности и прочих систем менеджмента в области информационной безопасности нередко приходится слышать применительно к модели Деминга – Шухарта фразу «волшебный цикл». По большому счету это не преувеличение, а лишь отражение того, что теория системного и процессного подходов попала в цель и практика многократно подтвердила эту теорию.

Рис. 14 иллюстрирует эталонную модель Деминга – Шухарта (модель Деминга), как это представляется экспертами технических комитетов ИСО, использующих данную модель в основе международных управленческих стандартов [8]. Эта методология в равной степени применима к высокоуровневым стратегическим процессам и простой операционной деятельности.

Основные фазы модели следующие:

– «планирование»: установление целей и процессов, необходимых для выработки результатов в соответствии с требованиями клиентов и политиками организации;

– «выполнение» («реализация»): реализация запланированных процессов и решений;

– «проверка»: контроль и измерение процессов и производимых продуктов относительно политик, целей и требований к продукции и отчетность о результатах;

– «действие» («совершенствование»): принятие корректирующих и превентивных мер для постоянного совершенствования функционирования процесса.

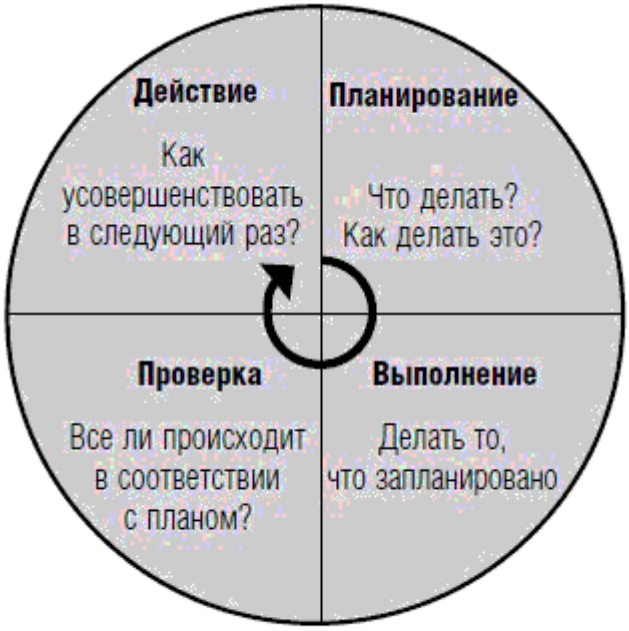


Рис. 14. Эталонная модель Деминга — Шухарта (модель Деминга)

В основе практики реализации модели Деминга лежит процессный подход. При этом само практическое наполнение понятия «процесс» не предполагает жесточайшей регламентации. В процессном подходе любая деятельность, которая выполняется или для управления которой используются ресурсы организации, считается процессом, преобразующим входы в выходы. Это методология (подход), идентифицирующая процессы в организации так, чтобы их взаимосвязи могли быть поняты, видимы и измеримы, а итоговая совокупность процессов понималась бы как единая система реализации целей деятельности организации (см. рис. 15).

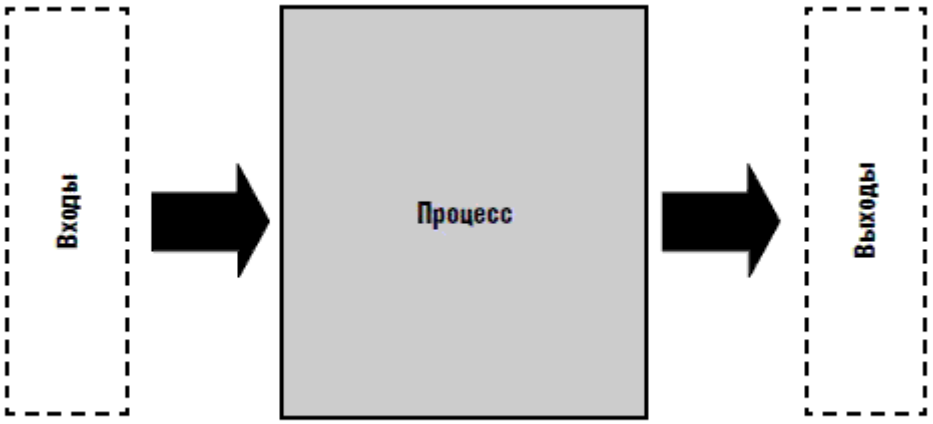


Рис. 15. Процессный подход

Процессный подход вводит горизонтальный менеджмент, пересекающий барьеры между различными функциональными единицами и консолидирующий их внимание на основных целях деятельности организации. Это не всегда берется в расчет и учитывается при принятии решения в организации о переходе на процессные технологии.

Как правило, структура организаций представляет собой иерархию функциональных единиц. Менеджмент организаций обычно осуществляется вертикально с разделением ответственности за намеченные результаты работ организации между функциональными единицами. Конечный потребитель или другая заинтересованная сторона не всегда отчетливо представляются всеми вовлеченными в работу сторонами (см. рис. 16). В результате проблемы, возникающие на границах сопряжения, часто считаются менее приоритетными, чем краткосрочные цели функциональных единиц (подразделений организации). Это ведет к незначительному совершенствованию для заинтересованных сторон или к полному отсутствию совершенствования, так как действия обычно сосредотачиваются на функциях, а не на общей пользе для организации и результатах ее деятельности.

Рис. 16. Пример процессной взаимосвязи через отделы организации

Оптимизация производственной инфраструктуры неизбежна при использовании процессного подхода, например перевода той или иной деятельности организации на стандарты процессного подхода. При этом и функционирование организации может быть усовершенствовано посредством использования процессного подхода. Осуществление менеджмента процессов в этих условиях такое же, как системы, – путем создания и осмысления сети процессов и их взаимодействий с идентификацией необходимых атрибутов процессной методологии (роли и ответственные, включая владение процессом, входы/выходы, работы процесса, показатели достижения целей и т. д.).

Выходы одного процесса могут быть входами для других процессов и могут быть связаны в общую сеть или систему процессов (см. общие примеры, приведенные на рис. 17 и 18).

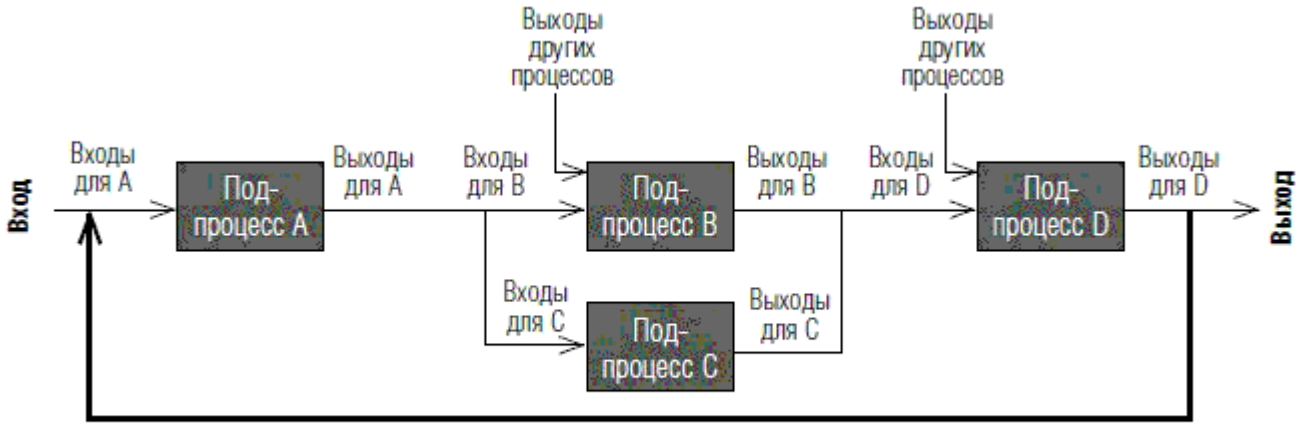


Рис. 17. Пример общей процессной последовательности

На практике качество решения задачи проектирования оптимальной и эффективной для данной организации сети или системы процессов предопределяет залог успеха всей компании использования процессной методологии. Здесь существует масса «подводных рифов», о которые может разбиться «корабль» реинжиниринга деятельности компании. Организационный аспект, отмеченный выше, есть один из них, который может застопорить все работы. Некоторые другие будут рассмотрены далее.

На уровне организации, как правило, выделяются следующие виды процессов (см. рис. 18):

– менеджмента организации – включают процессы, относящиеся к стратегическому планированию, установлению политик, постановке целей, обеспечению коммуникации, обеспечению доступности необходимых ресурсов и проверкам, проводимым руководством;

– менеджмента ресурсов – включают все процессы обеспечения ресурсов, которые необходимы для процессов менеджмента организации, реализационных процессов и процессов измерения;

– реализационные – включают все процессы, обеспечивающие намеченный выход для организации;

– измерения, анализа и совершенствования – включают процессы, необходимые для измерения и сбора данных для анализа функционирования и совершенствования эффективности и продуктивности, процессы измерения, мониторинга и аудита, корректирующие и превентивные меры и являются интегральной частью процессов менеджмента, менеджмента ресурсов и реализационных процессов.

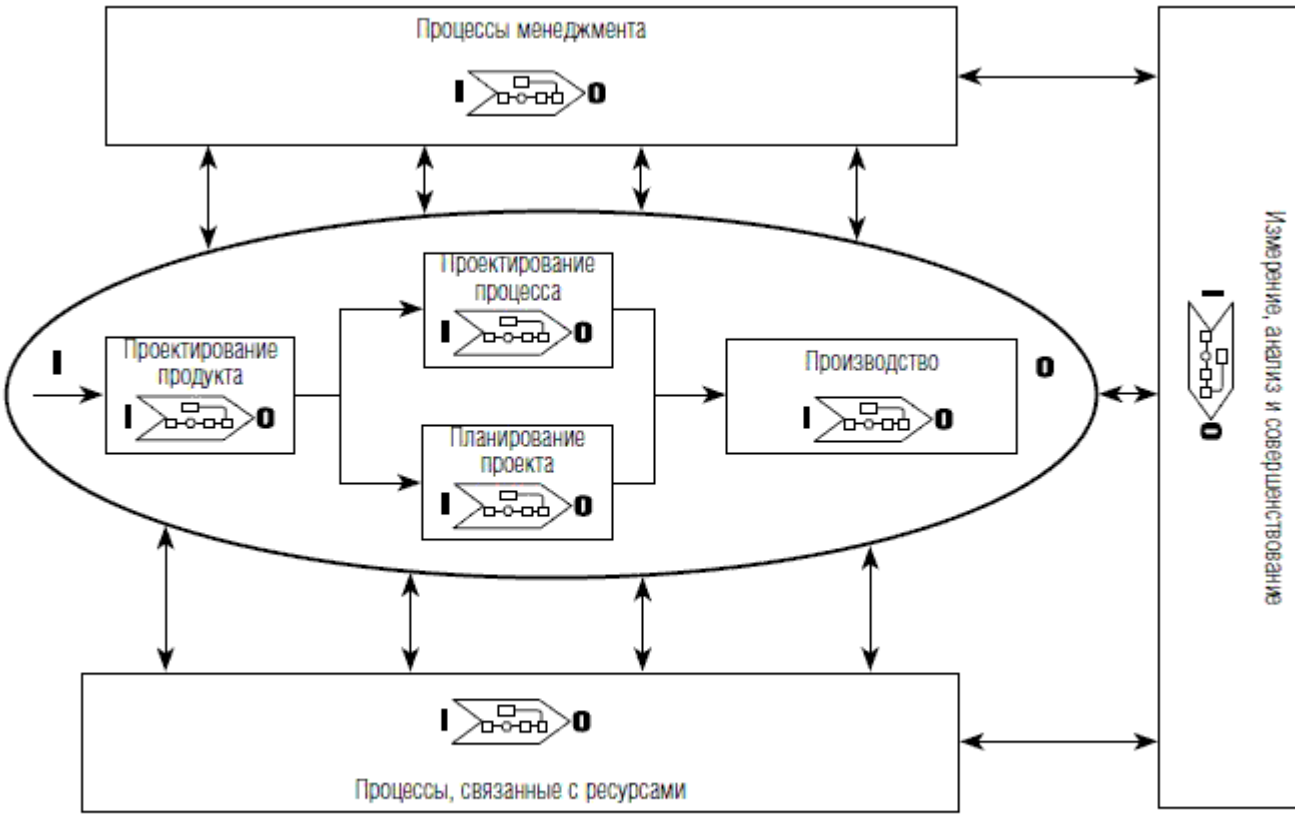


Рис. 18. Пример процессной последовательности и ее взаимодействий на уровне организации

Пример процессной последовательности и ее взаимодействий на уровне организации, представленный на рис. 18, иллюстрирует некую упрощенную эталонную модель, нуждающуюся в серьезной адаптации под операционную и управленческую инфраструктуру организации. Наиболее сложным в этой задаче, как правило, является вопрос регламентации действий (деятельности работников любого уровня), являющихся следствием внезапных или неожиданных событий (стохастическая составляющая в деятельности организации). В зависимости от рода деятельности организации, качества компонентов операционной среды и подготовки персонала стохастическая составляющая в деятельности организации может варьироваться от 20 до 80 %. Наиболее сложны в этом плане процессы менеджмента (управленческие процессы), связанные с принятием решений. Отдельные проблемы данной категории процессов, сопряженные с рисками принятия решений, затрагивались в предыдущей главе.

Эталонная реализация процессного подхода в рамках модели Деминга предполагает следующие пять основных процедурных шагов:

– идентификация процессов организации;
– планирование/проектирование процессов (для каждого реализуемого процесса);
– реализация процессов и измерения;
– анализ процессов;
– корректирующие действия и совершенствование процессов.

В связи с тем, что модель Деминга явно требует реализации контрольных процедур, основывающихся на объективных свидетельствах, отдельной проработки требует вопрос документирования, чтобы на практике заработал процесс «совершенствование» модели Деминга. Это включает то, что необходимо выполнить (требования и спецификации), и требования к документированию выполненной деятельности. При этом затруднительно организовать и еще сложнее поддержать в актуальном состоянии полный список документированных процессов организации и единый реестр требований к свидетельствам

выполненной деятельности. В то же время для целей измерений, контроля и аудита должны приниматься требования по документированию соответствующих результатов деятельности. Когда такие решения принимаются спонтанно и не согласованы с конечными производственными результатами, то вместо роста эффективности мы можем получить обратный результат, вплоть до деградации объекта рассмотрения.

Далеко за примерами ходить не надо. Известны результаты акций по внедрению систем менеджмента качества (СМК) в большинстве российских компаний, когда основной целью были «шашечки», а «ехать» никто никуда не собирался. Но это одна ситуация. Более печально, когда руководство организации на самом деле желает поднять качество деятельности (продукции), но в силу слабой компетенции сотрудников получает обратный результат… Даже для европейского менталитета и гораздо более высокой исполнительской дисциплины персонала западных компаний такая ситуации не редкость.

Журнал *European Quality,* издаваемый Европейской организацией по качеству, опубликовал в статье «10 аргументов против применения стандартов ИСО серии 9000» изложение фрагмента книги Дж. Седдона «В поисках качества. Дело против ИСО 9000» [9]. Автор считает, что существуют более надежные способы повышения эффективности предприятий, удовлетворения потребителей, обеспечения реального качества и увеличения прибылей, чем работа в соответствии с предписаниями стандартов ИСО серии 9000, даже в версии 2000 г. Дж. Седдон полагает, что внедрение стандартов ИСО серии 9000 нанесло ущерб конкурентоспособности сотен тысяч организаций. Он приводит мнение одного из британских специалистов, который был тесно связан с внедрением британского стандарта BS 5750, послужившего основой для разработки международных стандартов ИСО серии 9000: «Внедрение BS 5750/ISO 9000 в британской промышленности стало крупнейшим обманом». Автор отмечает, что главной ошибкой была излишняя уверенность организаций в том, что внедрение стандартов качества решит все проблемы (наивные британцы!). При этом обращается внимание на то, что процедура сертификации по ИСО 9000 не позволила организациям разглядеть реальные возможности для повышения своих показателей, которые они обязательно заметили бы в ином случае: процедура регистрации на соответствие стандартам ИСО 9000 заслонила собой эти возможности.

Среди аргументов против применения стандартов ИСО серии 9000 Дж. Седдон приводит и абсолютно ожидаемый, касающийся требований документирования СМК. Он отмечает, что из-за обилия отчетных регистрационных форм персонал компаний неявно подменяет ими содержание своего труда, так как контроль идет по формализованным свидетельствам о выполненной деятельности на том или ином участке работ. Ту же ситуацию мы видим и в российских компаниях, внедряющих подобные стандарты, когда их применение не ориентировано на совершенствование продукта/результата деятельности, когда решения о применении стандартов менеджмента не сопровождаются обсуждением и закреплением о том, что и как планируется улучшить в деятельности организации, относительно имеющейся в настоящее время ситуации.

2.1.3. Модели непрерывного совершенствования и международные стандарты

Указанные особенности и условия внедрения и применения модели Деминга уместны для любого вида менеджмента в организации (управленческого, производственного, обслуживающего, ресурсного и т. п.). Модель определяет основные этапы, шаги, а их наполнение – ту задачу, которую планируется решить. Все большее число принимаемых международных стандартов менеджмента для различных сфер их применения преследуют фактически одну главную цель – дать базовый ориентир содержательного наполнения работ модели Деминга в терминах и содержании решаемой задачи.

На рис. 19 и 20 представлены примеры структуры эталонной модели менеджмента применительно к эталонной модели менеджмент риска организации [10] и системы менеджмента информационной безопасности [11], обеспечивающие «настройку» модели

Деминга на соответствующие сферы применения.

Рис. 19. Компоненты структуры менеджмента риска в соответствии с ISO 31000

Структура менеджмента риска, представленная на рис. 19, предназначена для содействия организации в эффективном осуществлении менеджмент риска через реализацию соответствующего процесса менеджмента риска на различных уровнях и в рамках определенного контекста организации. Данная структура должна обеспечивать условия того, что полученная в результате работы из этих процессов информация о риске будет адекватным образом доведена до сведения и использована в качестве основы для принятия необходимых решений и поддержке отчетности на соответствующих уровнях корпоративного управления и операционной деятельности в организации.

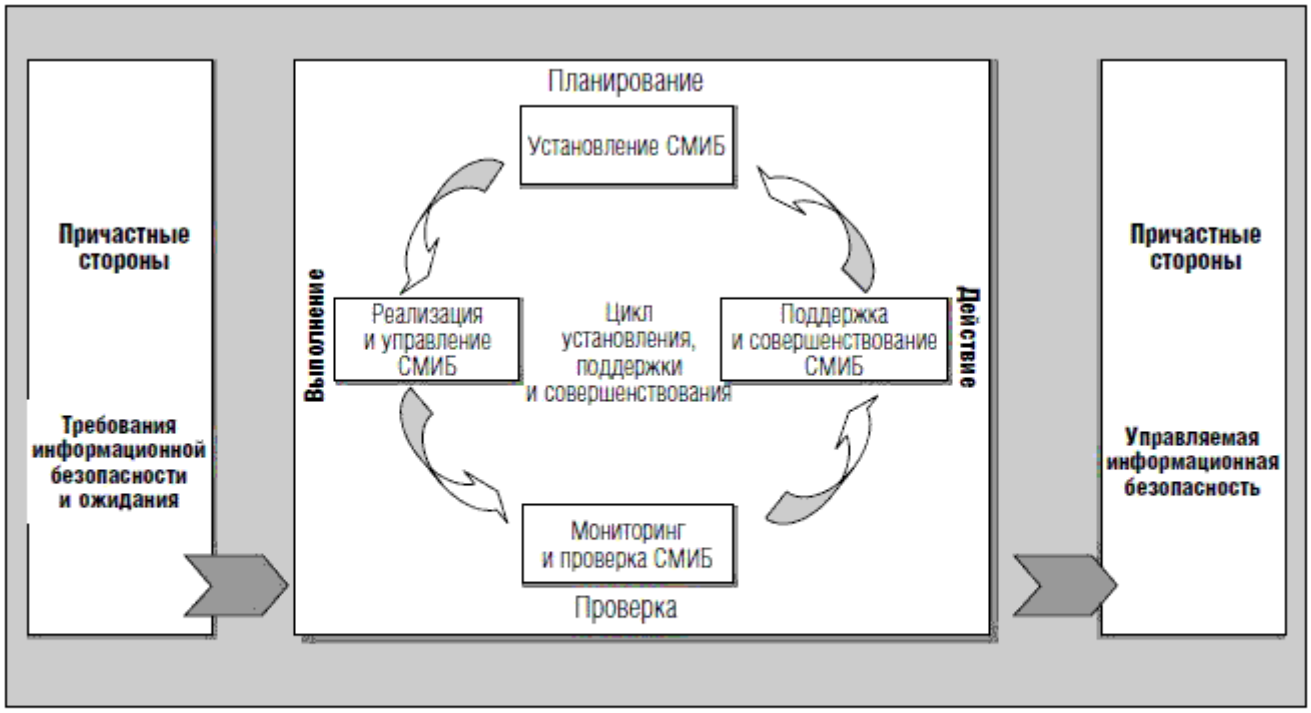


Рис. 20. Компоненты структуры системы менеджмента информационной безопасности организации в соответствии с ISO/IEC 27001

Структура менеджмента риска, представленная на рис. 20, предназначена для содействия организации в установлении и поддержке системы менеджмента информационной безопасности организации, отвечающей лучшим международным практикам. Далее будут достаточно подробно отражены шаги внедрения стандартизированных систем менеджмента информационной безопасности

Только приведенными примерами сфера применения моделей непрерывного совершенствования в структуре требований международных стандартов не ограничивается. К настоящему времени принято множество комплексов стандартов на системы менеджмента в различных сферах деятельности (от безопасности продуктов питания до управления цепочками поставок продукции), а также применительно к общим и отдельным задачам, реализуемым в рамках организаций.

Не вдаваясь в детали (с ними можно ознакомиться, взяв любой стандарт на ту или иную систему менеджмента), каждый из них (подобно приведенным на рис. 19 и 20) включает необходимые параметры настойки модели Деминга на соответствующие виды деятельности в терминах и семантике сферы применения. В целом же общий эталонный подход модели непрерывного совершенствования отражает рис. 21.

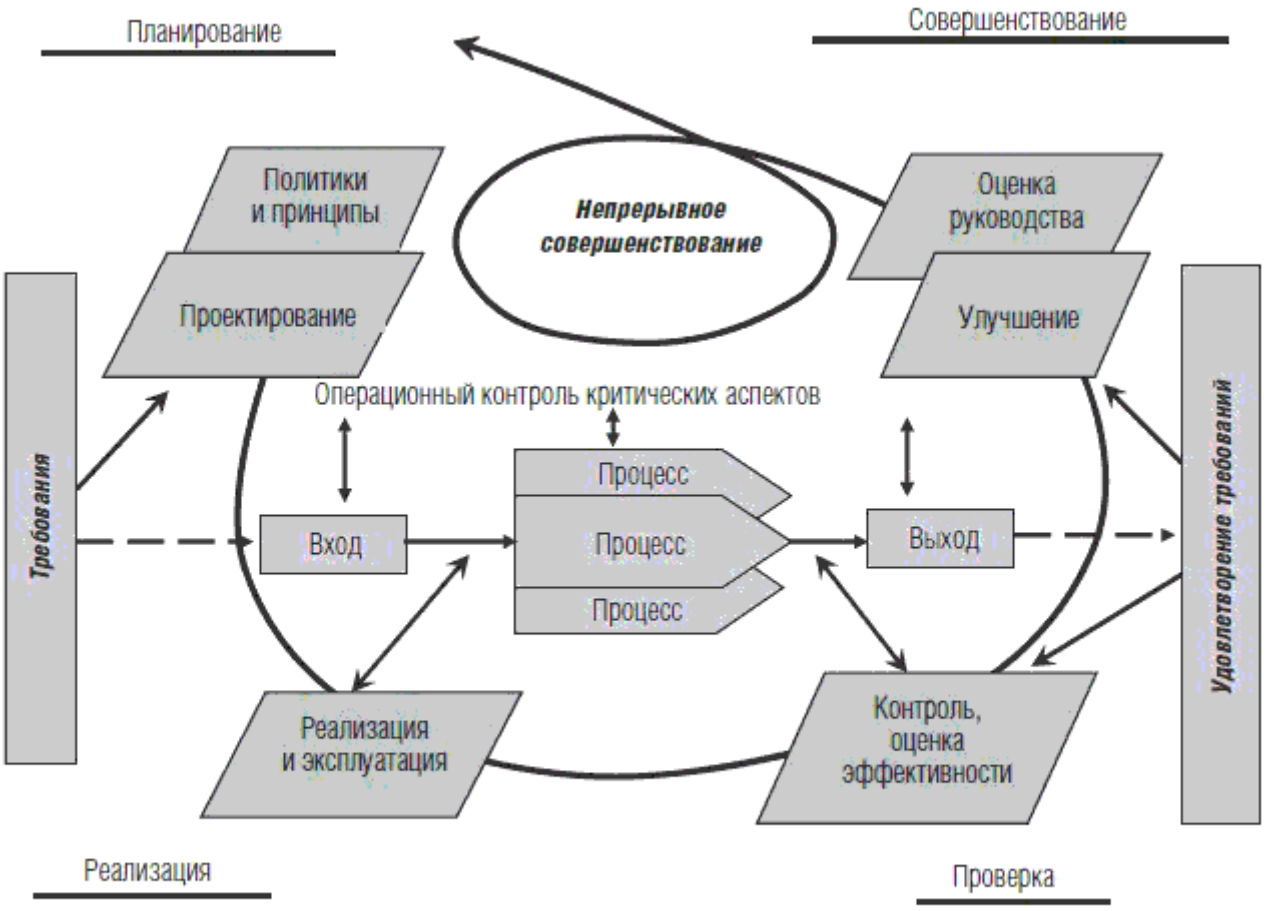


Рис. 21. Модель непрерывного совершенствования

Каждый из стандартов на системы менеджмента включает положения, де-факто ориентирующие на реализацию модели непрерывного совершенствования. Далее рассмотрим, как это может работать в рамках организации.

2.2. Стандартизированные модели менеджмента. Аспекты контроля и совершенствования. Интеграция

2.2.1. Стандартизированные модели менеджмента в системе корпоративного управления

На уровне организации любые стандартизированные решения на системы менеджмента попадают в одну среду и должны подчиняться единым нормам корпоративного управления. Рис. 22 иллюстрирует такую ситуацию на примере трех стандартизированных систем:

– менеджмента информационной безопасности организаций (ISO / IEC 27001);
– менеджмента качества (ГОСТ Р ИСО 9000);
– менеджмента окружающей среды (ГОСТ Р ИСО 14000).

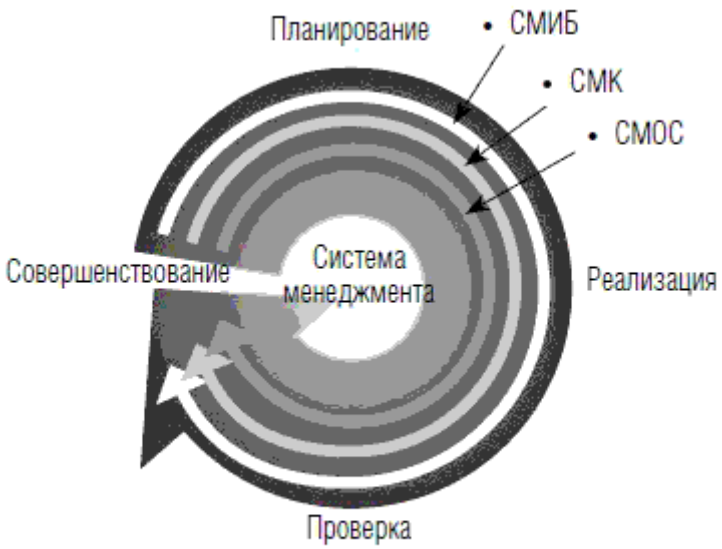
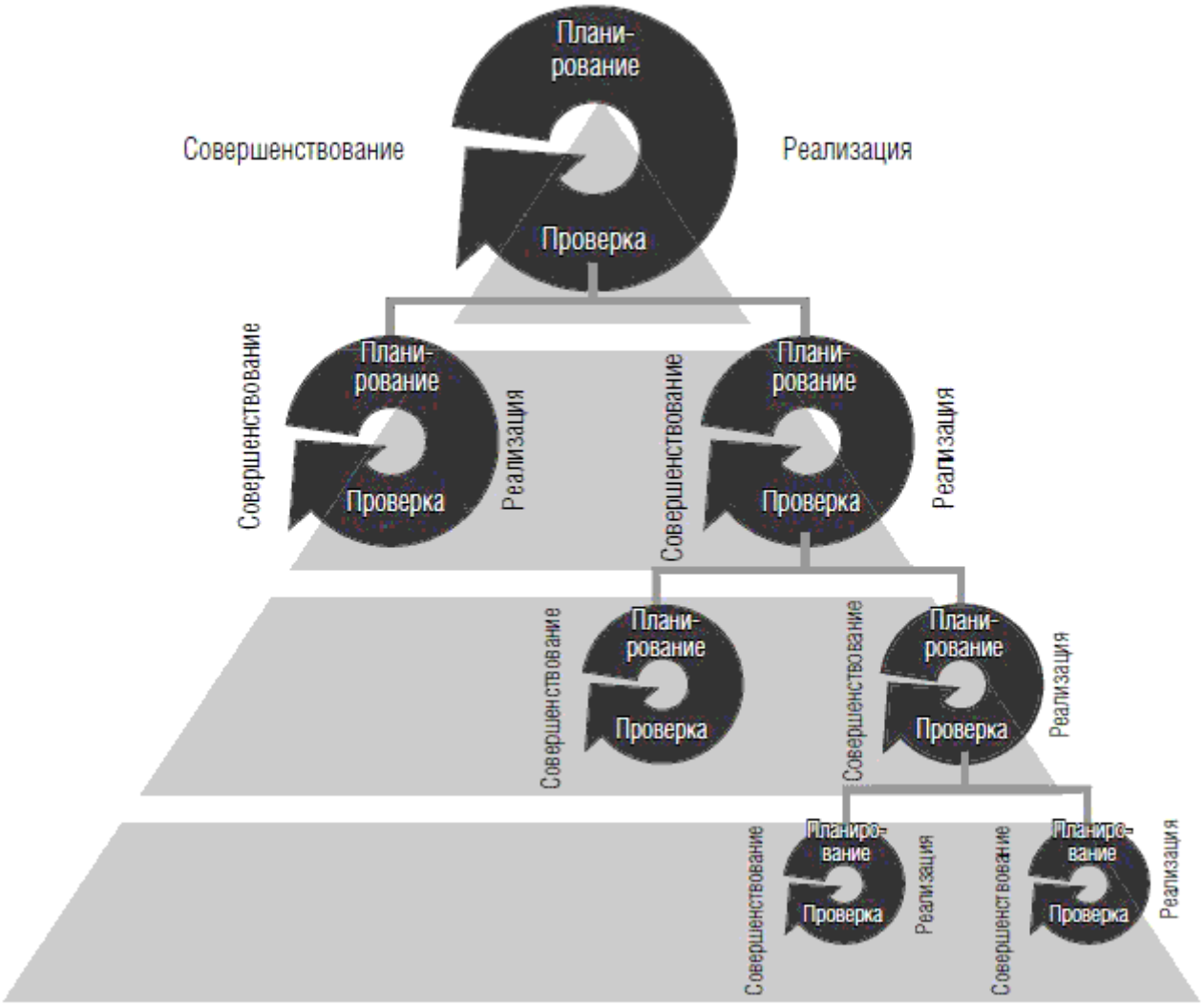


Рис. 22. Объекты системы менеджмента

Перечисленные системы менеджмента косвенно поддерживают менеджмент всех бизнес-процессов (пример рассматривает «вспомогательные»/«обеспечивающие» виды деятельности) как часть корпоративной системы, менеджмента риска в частности, для достижения организацией установленных целей. С точки зрения корпоративного управления эта модель должна иметь поддержку на соответствующих уровнях управления, как показано на рис. 23.



Системы менеджмента для более низких уровней работают во взаимодействии с системами менеджмента для более высоких уровней. На каждом из уровней корпоративного управления (будь то самостоятельно юридическое лицо или подразделение организации) должны учитываться все аспекты и сферы деятельности, как это определяется вышестоящим уровнем управления, включая свою часть (в рамках полномочий и ответственности) по планированию/проектированию, исполнению, контролю и выработке предложений/решений совершенствования деятельности.

Рис. 24 иллюстрирует возможную организацию реализации процессов СМИБ при двухуровневой организации деятельности компании. Каждый из уровней управления должен поддерживать отвечающие его функциям процессы СМИБ, соответствующие сферам ответственности правам и обязанностям каждого из уровней управления.

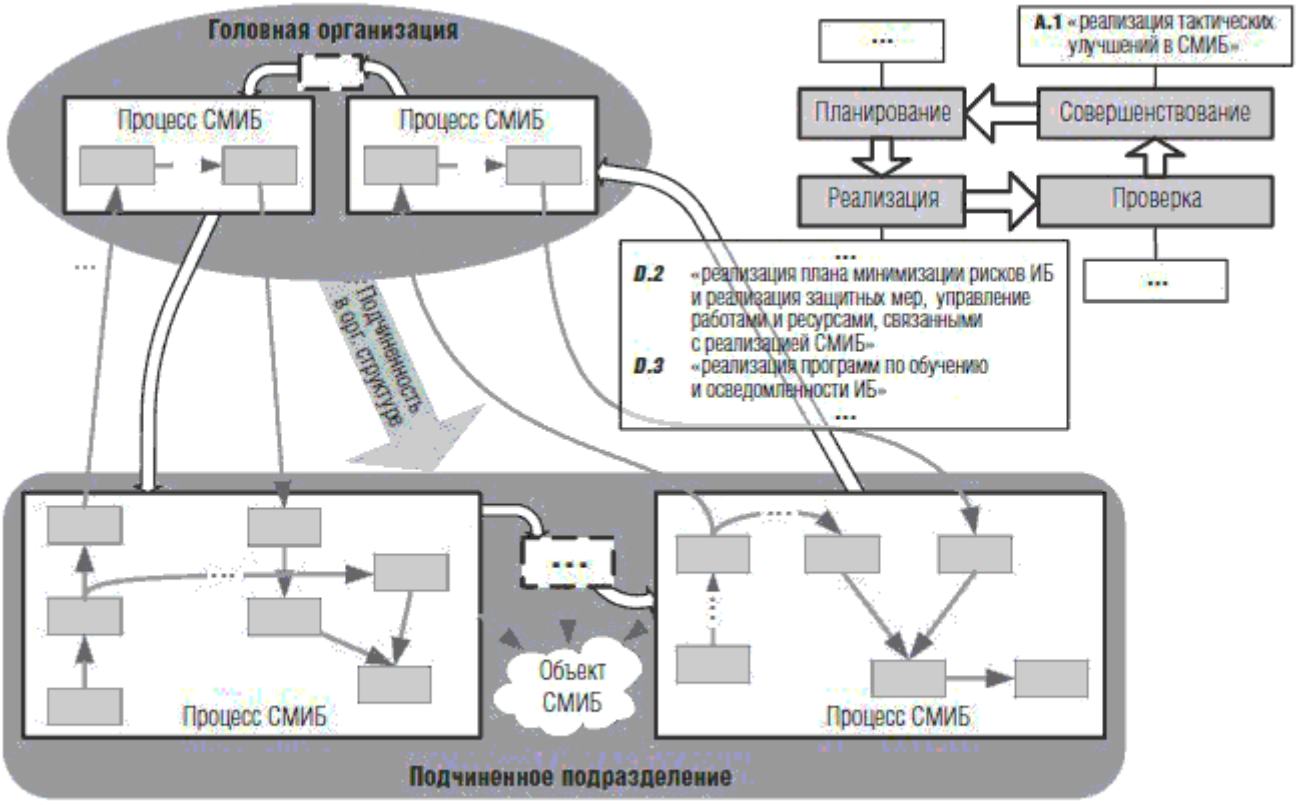


Рис. 24. СМИБ при двухуровневой организации деятельности компании

В приведенном примере для процессов планирования работ, принятия решений о целях и задачах СМИБ, владельцами будут сотрудники головной организации компании, а исполнительская и первичная контрольные виды деятельности будут реализованы на уровне подчиненного подразделения. Общий (итоговый) контроль, конечно же, ляжет на корпоративный центр. Процессы совершенствования деятельности в такой организации деятельности должны иметь критерии тактических (в рамках полномочий руководства подчиненных подразделений) и стратегических (компетенция принятия решений за головной организацией) решений.

Реализация других системы менеджмента в рамках компании будет подразумевать подобную организацию и реализацию процессов деятельность, так как будет осуществлена в той же системе внутрикорпоративных правил.

Важнейшая роль руководства (высшего руководства) организации с точки зрения эффекта внедрения и результатов внедрения любых стандартов менеджмента отмечается практически во всех стандартах.

Например, в ISO/IEC 27001 [11]:

«Руководство должно предоставлять свидетельства исполнения своих обязательств по установлению, реализации, приведению в действие, мониторингу, проверке, поддержке и совершенствованию системы менеджмента информационной безопасности путем:

а) установления политики системы менеджмента информационной безопасности;

б) обеспечения установления целей системы менеджмента информационной безопасности и планов;

в) установления ролей и обязанностей, связанных с информационной безопасностью;

г) доведения до персонала организации о важности выполнения целей информационной безопасности и соблюдения политики информационной безопасности, об обязанностях в соответствии с законом и о потребности в постоянном совершенствовании;

д) предоставления достаточных ресурсов для установления, реализации, приведения в действие, мониторинга, проверки, поддержки и совершенствования системы менеджмента

информационной безопасности;

е) вынесения решения о критериях принятия риска и приемлемых уровнях риска;

ж) обеспечения проведения внутренних аудитов системы менеджмента информационной безопасности;

з) осуществления проводимых руководством проверок системы менеджмента информационной безопасности».

Только высшее руководство компании имеет полномочия по определению уровня (порогов) для принятия рисков. Вопрос порядка обсуждения и принятия решений по порогам риска крайне специфичен для каждой организации. Это обусловлено тем, что именно руководство несет окончательную ответственность за инвестиции в СМИБ и ее эффективность и, следовательно, эффективность инвестиций организации по данной статье расходов. В этих условия стандарты выступают в качестве некоторого возможного эталона действий, но не как истина в последней инстанции. Руководство компаний находится в некотором смысле в многомерном пространстве, где оно должно сориентироваться, оценить каждый вектор и принять необходимое по ситуации решение. Рис. 25 иллюстрирует основные плоскости такого пространства для задач обеспечения ИБ.

Рис. 25. Основные срезы корпоративного управления информационной безопасности бизнеса

Целями обеспечения учетности для сферы безопасности могут быть:

Три основные цели корпоративного управления информационной безопасностью

– обеспечение подотчетности совету директоров;

– определение ответственности и обеспечения разделение обязанностей;

– выделение требуемого объема ресурсной базы;

– обеспечение осведомленности о защищенности бизнеса.

Целями обеспечения потребностей бизнеса в сфере безопасности могут быть:

– установление соответствия ИБ стратегии бизнеса организации;

– базирования основных решений в сфере безопасности на результатах менеджмента риска;

– обеспечение уверенности в том, что СМИБ охватывает вопросы безопасности бизнес-процессов (процессов деятельности).

Целями обеспечения соответствия (для любого вида деятельности) могут быть:

– исполнение требований действующего законодательства и норм, имеющих отношение к информационной сфере и деятельности организации;

– исполнение в операционной среде организации принятых советом директоров и высшим исполнительным руководством внутренних нормативных документов.

Применительно к иным сферам (отмечавшимся менеджменту качества и экологии, а также к иным видам менеджмента в организации, таким как менеджмент ИТ-услуг, менеджмент риска, менеджмент цепочек поставки, менеджмент активов и т. п.), как правило, стоит схожая задача, и пространство корпоративных решений подобно за исключением своей специфичной семантики.

Вопросы обеспечения соответствия (соответствия законодательным и нормативным требованиям) – здесь меньшая, но также не всегда прозрачная составляющая. Что же касается соответствия потребностям бизнеса в вопросах защищенности, то это, как правило, на порядок большая проблема.

Обусловлена она не только и не столько сложностью проблемы идентификации опасностей бизнеса (о чем достаточно подробно было обсуждено в предыдущей главе) и выбора соответствующих мер защиты, сколько нахождением общего языка внутри организации (общего языка и алфавита общения) между бизнесом и безопасностью, внутренним контролем и информатизацией, безопасностью и внутренним контролем. Консолидирующим органом в этих условиях может выступать только лишь высшее руководство организации (внешний компетентный арбитр), несущее ответственность перед собственниками бизнеса (владельцами организации/компании) за результаты деятельности организации.

Однако, даже если высшее руководство понимает и принимает ответственность за систему менеджмента в организации, у него нет возможности участия во всех мероприятиях. По этой причине руководство должно первоначально установить политику системы менеджмента информационной безопасности, определяющую основные цели и ожидания от СМИБ с точки зрения совершенствования деятельности организации, тем более если внедряется «стандартизированная» СМИБ. «Нестандартизированная СМИБ» существует в любой организации (принимаются решения и внутренние нормативы, осуществляются инвестиции в ИБ, осуществляется контроль исполнения требований и т. д.). Это следует понимать и учитывать в проектах модернизации.

Например, в рамках инвестиций в информационные технологии многие организации явно или неявно осуществляют внедрение ряда функций и механизмов, имеющих отношение к обеспечению ИБ. Далее, организуя их использование в составе прикладных систем или информационно-телекоммуникационной инфраструктуры организации, де-факто осуществляются те или иные практические задачи, подпадающие под положения стандартов требований к СМИБ.

Схематично данную ситуацию иллюстрирует рис. 26, отражающий в упрощенном виде категории управления в информационной сфере организации.

Рис. 26. Категории управления в информационной сфере организации

И корпоративное управление информационными технологиями, и корпоративное управление информационной безопасностью являются неотъемлемой частью корпоративного управления компании, имеющие как общности (общие факторы: объекты, предметы, отношения и т. п.), так и различия. Опыт, накопленный в последние десятилетия, позволил подойти к выработке и принятию международных модельных стандартов корпоративного управления информационными технологиями.

Рис. 27 иллюстрирует модель корпоративного управления ИТ, рекомендуемую принятым в 2008 г. международным стандартом ISO/IEC 38500 «Корпоративное управление информационными технологиями» [12].

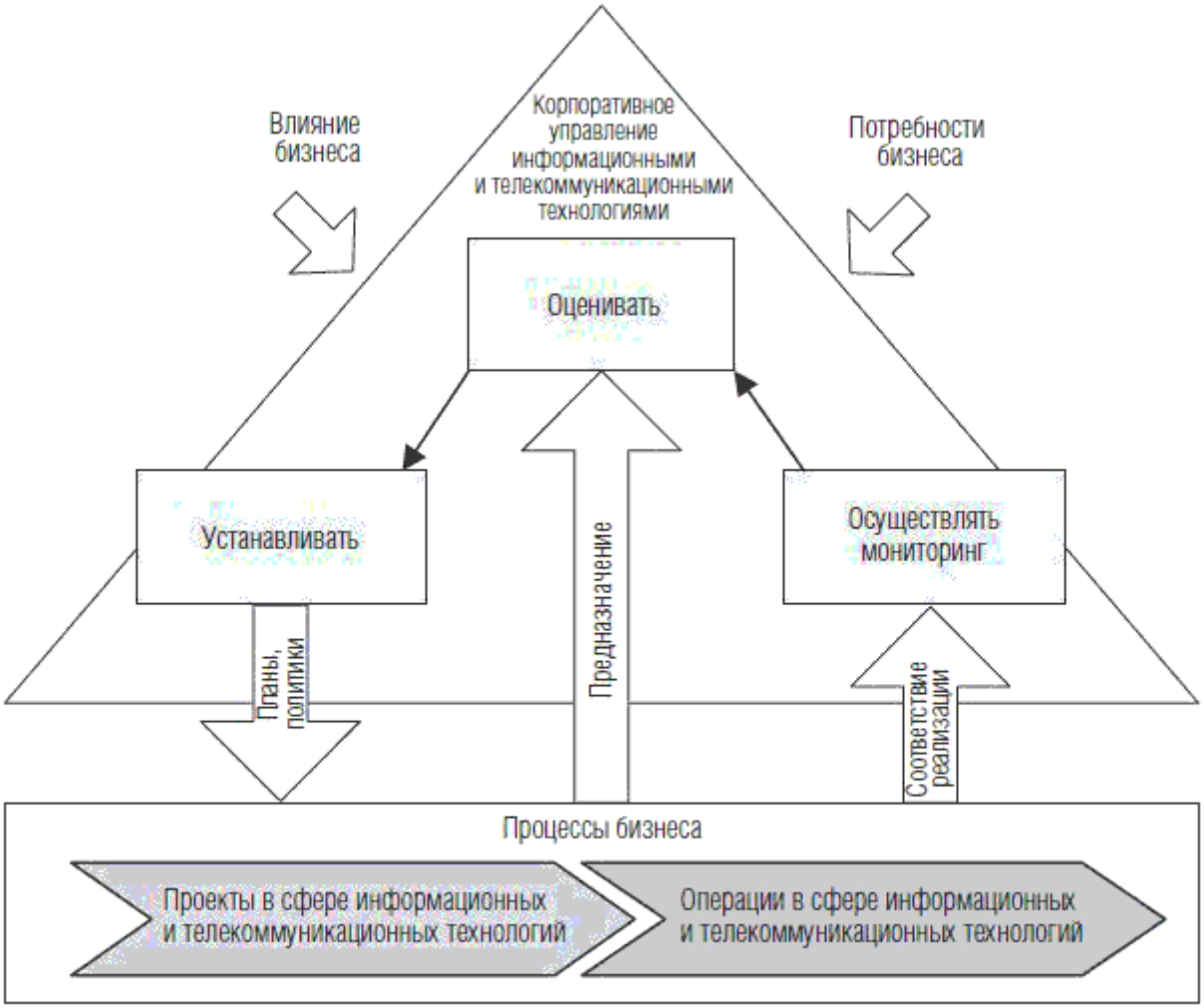


Рис. 27. Модель корпоративного управления ИТ в соответствии с ISO/IEC 38500

Модель корпоративного управления ИТ, представленная на рис. 27, отражает тот факт, что в любой деятельности организации изначально присутствует этап инвестиций (в той или иной форме), в результате которого организация ожидает, что эти инвестиции принесут пользу и дадут положительный эффект. Применительно к корпоративному управлению ИТ это включает:

– проекты организации в сфере информационных и телекоммуникационных технологий – этап инвестиций в операционную ИТ-среду;

– операции в сфере (эксплуатация поставленных) информационных технологий организации – этап возврата инвестиций. В сфере информационных технологий возврат инвестиций может быть представлен в виде: новой функциональности организации (подразделений), повышения надежности и безопасности систем информационных технологий и информационной составляющей процессов деятельности, сокращения эксплуатационных издержек и т. п.

Возможно, подобные модельные рекомендации будут приняты и для сферы корпоративного управления информационной безопасностью, включая место и роль стандартизированных требований к СМИБ в системе корпоративного управления. На рис. 28 представлена возможная модель корпоративного управления информационной безопасностью организации, согласующаяся с признанной моделью корпоративного управления информационными технологиями в организации, нашедшей отражение в ISO / IEC 38500.

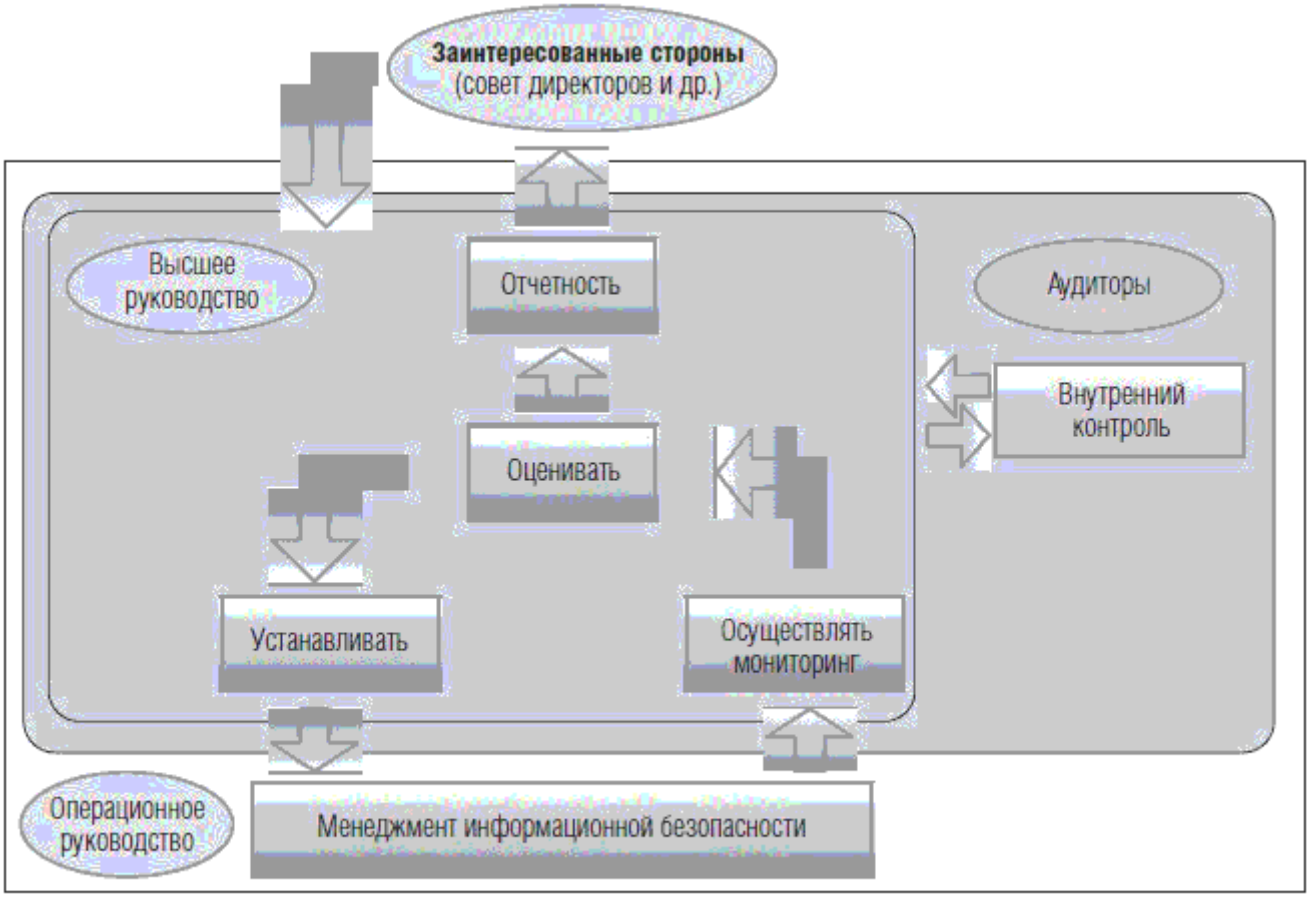


Рис. 28. Возможная модель корпоративного управления информационной безопасностью организации

В любом случае должны быть идентифицированы роли и функции органов управления компании и вопросы смежных областей. Одно из возможных модельных решений применительно к архитектуре корпоративного управления информационной безопасностью представлено на рис. 29.

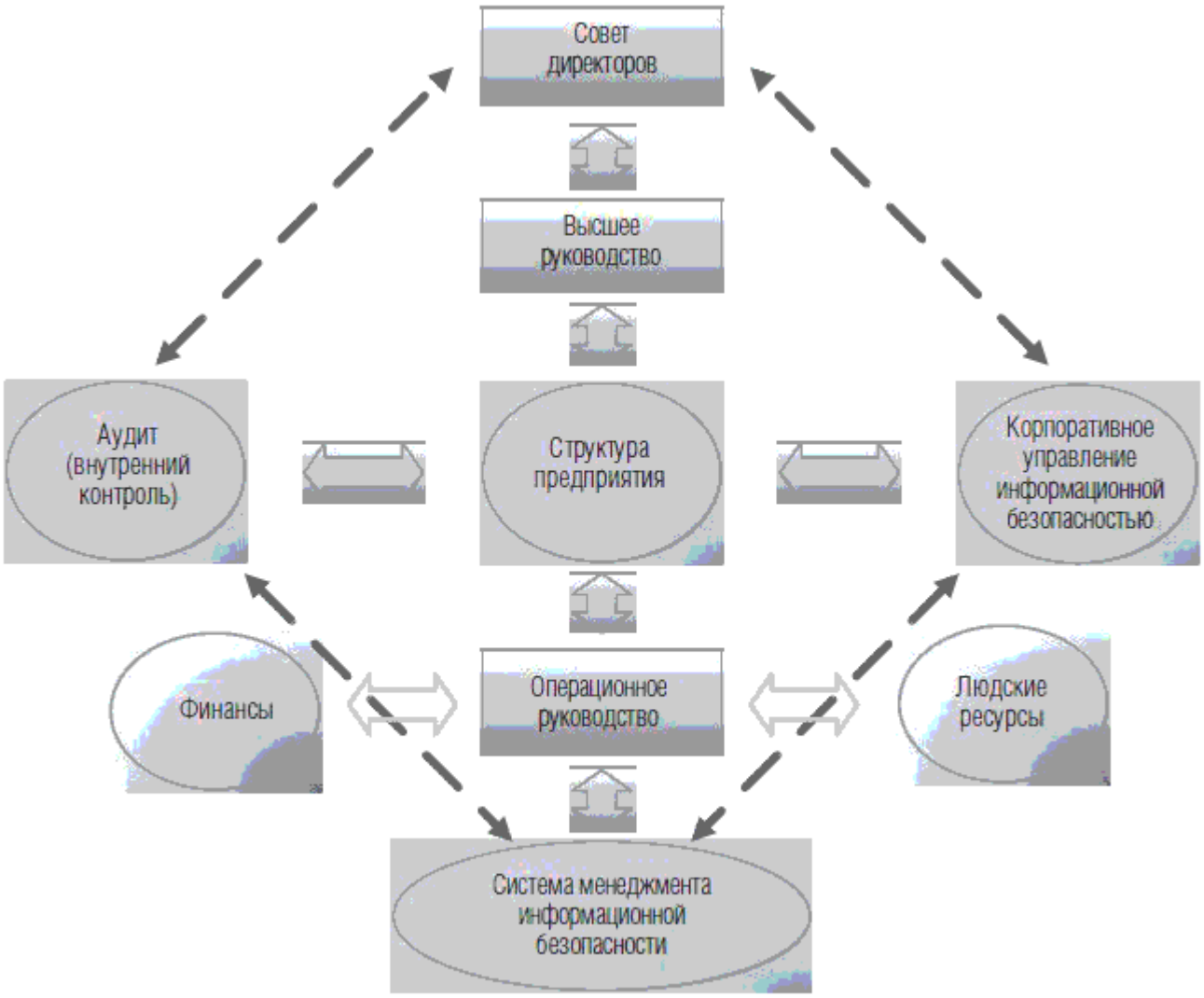


Рис. 29. Архитектура корпоративного управления информационной безопасностью

В конечном итоге наиболее критичным вопросом и одной из важнейших задач высшего руководства является обеспечение таких бизнес-ресурсов, как «люди», «предметы» и «деньги». В конечном итоге успех дела (в данном случае эффективность затрат в СМИБ организации), как и в традиционном бизнесе, будет зависеть от достаточности ресурсной поддержки. При этом крайне чувствительным и одновременно сложным здесь является вопрос о достаточности ресурсной поддержки (как установить порог/критерий, характеризующий, что «все заработало»). Современные стандарты СМИБ включают такие формулировки: *руководство должно понимать потребности системы менеджмента информационной безопасности и предоставлять для нее необходимые бизнес-ресурсы.*

Однако значение того, сколько составляет «необходимое» и «достаточное», стандартами установлено быть не может. Есть «микро» предприятия, есть средние и большие. При этом градации сегментов: малое предприятие, среднее и большое – в некоторой степени абстрактны и имеют различия от вида и сферы деятельности (бизнеса) организации. В различных странах (и в России, в частности) существует формальное определение малого предприятия для целей льготного налогообложения, но это все-таки достаточно условная градация, с порогами, устанавливаемыми от годового дохода компании. В то же время с развитием технологий и вынужденной унификацией отдельных задач данные абстрактные критерии все же получают вполне возможное содержанием для отдельных областей.

Например, в сфере информационных технологий в начале 2000-х гг. стал формироваться срез (где-то клон) стандартов информатизации для объектов, получивших

наименование «очень малая организация (предприятие)» (Very Small Enterprises (VSE)). С практической точки зрения это вполне оправдано: в мире многим миллионам микрокомпаний (а это тот срез экономики, что генерирует несколько десятков процентов всего мирового ВВП) требуется иметь автоматизированную бухгалтерию, выход в Интернет (электронная почта, электронные торги и т. п.), автоматизированный учет кадров и т. п. При этом классические полные циклы инвестиций в информатизацию и их возврата, а также классика менеджмента информационными технологиями, процессами жизненного цикла систем и программных средств со всеми вытекающими атрибутами для них «неприподъемны». В будущем, возможно, и в сфере требований к СМИБ организаций и задачам корпоративного управления ИБ будет обращено внимание к сегменту VSE. Однако область безопасности чрезвычайно чувствительная и специфичная и консенсус здесь найти не так-то просто. Многие защитные меры ИБ в организациях сегмента VSE реализуются механизмами бизнеса (доверие, гарантии, страхование, аутсорсинг). Такие решения сложно облачить в форму универсальных стандартов СМИБ для VSE.

2.2.2. Универсальные требования к стандартам на системы менеджмента

Все опубликованные стандарты на системы менеджмента отвечают единым принципам их назначения, структуры требований и содержания. Это обеспечивается едиными правилами и нормами, действующими в рамках международной организации по стандартизации (ИСО).

Технический административный совет ИСО, осознав потребность в обеспечении совместимости стандартов систем менеджмента и признав, что этому может способствовать единая методология принятия решений и разработки таких стандартов, подготовил ряд модельных типовых решений. В результате в качестве дополнительных требований к действующим административным директивам ИСО/МЭК было разработано руководство по обоснованию и разработке стандартов систем менеджмента, изданное в 2001 г. как Руководство ISO 72 [13].

Основным назначением подготовленных рекомендаций являлось создание условий для обеспечения сопоставимости и совместимости, упрощения совместного использования стандартов систем менеджмента организациями, желающими одновременно следовать положениями более чем одного стандарта на системы менеджмента.

По назначению Руководство ISO 72 является дополнением к процедурам для технической работы и методологии разработки международных стандартов, устанавливаемым директивами ISO/IEC, определяющим ряд общих требований к работе технических комитетов ISO, планирующих разработку или разрабатывающих стандарты менеджмента. Эти общие нормы и формируют совместимость стандартов менеджмента по ключевым сущностям, стратегиям внедрения и развития. Все присутствующие на рынке услуг предложения по внедрению в организациях так называемых «интегрированных систем менеджмента» в своей основе опираются на Руководство ISO 72, дополняя его специфичной семантикой, отражающей, сколько систем менеджмента планируется одновременно «загрузить» в систему корпоративного управления организации.

В целом Руководство ISO 72 рекомендует выделять три следующих вида стандартов систем менеджмента.

– А – *стандарты требований* системы менеджмента как общие, так и характерные для сектора;

– Б – *стандарты рекомендаций* для системы менеджмента как общие, так и характерные для сектора;

– В – *стандарты, связанные* с системой менеджмента.

Стандарты вида А (стандарты требований системы менеджмента) предназначены для формирования соответствующих спецификаций менеджмента, позволяющих осуществлять

оценку для демонстрации соответствия внутренним и внешним требованиям (например, путем независимой оценки первой, второй или третьей стороной). Примерами таких стандартов являются:

– стандарты требований системы менеджмента (спецификации), например ISO/IEC 27001, ИСО 9001 и т. п.;

– характерные для сектора стандарты требований системы менеджмента;

– стандарты по аккредитации органов оценки и сертификации систем менеджмента.

Стандарты вида Б (стандарт рекомендаций для системы менеджмента) предназначены для оказания содействия организации в реализации и /или улучшении системы менеджмента путем предоставления дополнительного руководства по элементам стандарта требований системы менеджмента. Примеры таких стандартов:

– руководство по использованию стандартов требований системы менеджмента;

– руководство по установлению системы менеджмента;

– руководство по совершенствованию/улучшению системы менеджмента;

– характерные для сектора стандарты рекомендаций для системы менеджмента.

Стандарты вида В (стандарт, связанный с системой менеджмента) предназначены для обеспечения дополнительной информации по определенным компонентам системы менеджмента или руководствам по взаимосвязанным поддерживающим методам и средствам, являющимся полезным и востребованным дополнением к положениям стандартов на системы менеджмента. Примеры таких стандартов:

– документы по терминологии системы менеджмента;

– стандарты руководств по аудиту, документированию, обучению, мониторингу, измерениям и оцениванию функционирования;

– стандарты по маркировке и оценке жизненного цикла.

Комплекс стандартов, имеющих с своем составе стандарты систем менеджмента типов А, Б и В, рекомендуется рассматривать как семейство стандартов менеджмента. Например, для систем менеджмента информационной безопасности к 2010 г. уже фактически сформировалось семейство стандартов СМИБ, отвечающее требованиям Руководства ISO 72 (см. рис. 30).

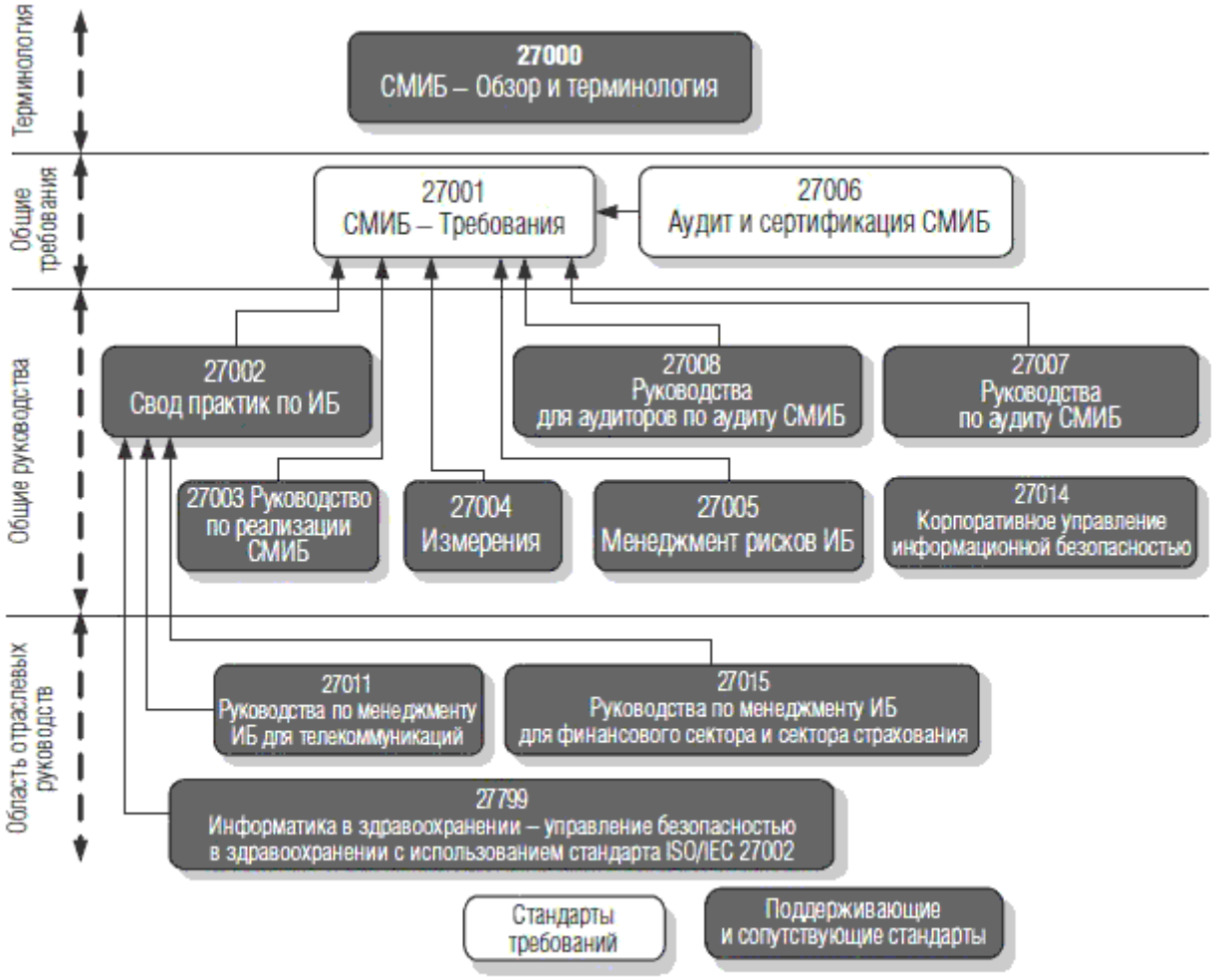


Рис. 30. Семейство стандартов СМИБ

Совместимость стандартов требований системы менеджмента или стандартов рекомендаций для системы менеджмента и простоту использования их предполагается улучшить посредством увеличения общности между стандартами, разрабатываемыми в соответствии с положениями Руководства ISO 72. Общность стандартов основывается на следующих общих составляющих стандартов:

– модель системы менеджмента;
– структура стандарта;
– система общих элементов вместе с их формулировкой;
– используемая терминологии.

Модель и структура. Общая структура стандарта требований системы менеджмента или рекомендаций для системы менеджмента основывается на признанной модели (модели Деминга) и логике системы требований (спецификации) к системе менеджмента в соответствии с данной моделью. В Руководстве ISO 72 отмечается, что в настоящее время в международных стандартах менеджмента используются две признанные модели: модель Деминга (PDCA) и процессная модель. Однако это не означает, что существующие модели для стандартов систем менеджмента будут с течением времени развиваться, и могут появиться новые модели.

Общие элементы. В Руководстве ISO 72 отмечается, что опыт работы со стандартами систем менеджмента, созданными ИСО, показывает, что практика работ выводит на ряд общих областей систем менеджмента. Такими общими областями предлагается считать:

– политику системы менеджмента;
– планирование;

– реализацию и введение в действие;
– оценку функционирования;
– совершенствование;
– проверки, проводимые руководством.

Боле подробно данные общие элементы представлены в таблице 1.

Общие элементы стандартов систем менеджмента ИСО

Таблица 1

Общие элементы стандартов систем менеджмента ИСО

Общие области	Общие элементы	Типично охватываемые вопросы
Политика	Политика и принципы	Политика для демонстрации приверженности организации выполнению требований, связанных со стандартом системы менеджмента, и установления общего понимания направления и принципов действия. Политика должна обеспечивать структуру для установки целей и задач
Планирование	1. Идентификация потребностей, требований и анализ критических вопросов.	1. Идентификация вопросов, которые должны контролироваться и /или совершенствоваться с целью удовлетворения соответствующей заинтересованной стороны (сторон). Термин «требования» включает и юридические требования.
	2. Выбор существенных вопросов для рассмотрения.	2. Расстановка задач, идентифицированных в результате шага 1, в соответствии с их приоритетами.
	3. Установление целей и задач.	3. Идентификация четких целей и задач (включая временные рамки) на основе результатов шага 2, политики организации и результатов проверки, проводимой руководством.
	4. Идентификация ресурсов.	4. Идентификация необходимых ресурсов и доступности адекватных кадровых, инфраструктурных и финансовых ресурсов.

Продолжение табл. 1

Общие области	Общие элементы	Типично охватываемые вопросы
	5. Идентификация организационной структуры, ролей, обязанностей и полномочий.	5. Идентификация ролей, обязанностей, полномочий и их взаимосвязей в организации, которые необходимы для обеспечения эффективных и результативных операций.
	6. Планирование операционных процессов.	6. Планирование механизмов операционных процессов, которые могут включать действия, влияющие на то, как достичь целей и задач, определенных на шаге 2.
	7. Готовность к обеспечению непрерывности при предсказуемых событиях	7. Механизмы, которые должны существовать, чтобы справляться с предсказуемыми чрезвычайными ситуациями
Реализация и введение в действие	1. Операционный контроль.	1. Меры операционного контроля, необходимые для реализации плана (планов) и поддержки контроля мероприятий относительно определенных целей.
	2. Менеджмент кадровых ресурсов.	2. Менеджмент кадровых ресурсов: служащих, подрядчиков, временного персонала и т. д. (включая квалификации и такие мероприятия, как формирование осознания и обучение).
	3. Менеджмент других ресурсов.	3. Операционный менеджмент и поддержка инфраструктуры, оборудования, мощностей, финансов и т.д., которые оказывают влияние на функционирование организации.
	4. Документация и ее контроль.	4. Менеджмент документов, которые важны для успешной реализации и действия системы менеджмента.
	5. Обмен информацией.	5. Механизмы связи внутри организации, направление информации внешним источникам и принятие ее от них.
	6. Взаимосвязи с поставщиками и подрядчиками	6. Оформление договоров с теми, кто поставляет и привлекается на выполнение услуг для организации, оказывающих влияние на функционирование организации
Оценка функционирования	1. Мониторинг и измерения.	1. Механизмы, с помощью которых организация постоянно оценивает свое функционирование.
	2. Анализ и разрешение несоответствий.	2. Определение несоответствий и способов их разрешения.
	3. Аудиты системы	3. Аудит системы менеджмента

Окончание табл. 1

Общие области	Общие элементы	Типично охватываемые вопросы
Совершенствование	1. Корректирующие меры.	1. Механизм устранения причин обнаруженных несоответствий как в системе менеджмента, так и в операционных процессах.
	2. Превентивные меры.	2. Механизм побуждения действий для устранения потенциальных причин несоответствий как в системе менеджмента, так и в операционных процессах.
	3. Постоянное совершенствование	3. Меры, принятые для обеспечения постоянного совершенствования системы менеджмента
Проверки, проводимые руководством	Проверки, проводимые руководством	Проводимая руководством проверка системы для определения ее текущего функционирования, контроля адекватности ее и эффективности, принятие решений и распоряжений об усовершенствованиях и новых направлениях, если это необходимо

Таблица 1 показывает общие элементы стандартов требований системы менеджмента и стандартов рекомендаций для системы менеджмента ИСО, перечисленные в соответствии с этой структурой. Разработчиками стандартов системы менеджмента рекомендуется соблюдение представленной в Руководстве ISO 72 системы элементов для облегчения использования стандартов, а также совместной реализации стандартов систем менеджмента. При этом ими рекомендуется также использование подобных (схожих) формулировок при составлении текстов для общих элементов стандартных требований к системам менеджмента.

2.2.3. Шаги реализации стандартной СМИБ организации

Стандартной СМИБ присущи все общие для систем менеджмента элементы. При этом опыт использования стандартизированных требований к СМИБ показал, что следующие факторы часто оказываются решающими для успешной реализации обеспечения информационной безопасности в организации:

– политика информационной безопасности, цели и мероприятия, отражающие цели бизнеса организации;

– подход и структура для реализации, поддержки мониторинга и совершенствования информационной безопасности, согласующиеся с культурой организации;

– явная поддержка и приверженность руководства всех уровней;

– хорошее понимание требований ИБ, оценки риска и менеджмента риска;

– эффективные мероприятия по осведомленности по вопросам ИБ для достижения должного осознания;

– распространение руководств (инструкций) по политике и стандартам информационной безопасности среди всех руководителей, служащих и других сторон;

– обеспечение финансирования мероприятий менеджмента ИБ;

– обеспечение соответствующей информированности, обучения и образования;

– установление эффективного процесса менеджмента инцидентов информационной безопасности;

– реализация оценивания системы, которое используется для оценок эффективности

функционирования менеджмента информационной безопасности и предложений по совершенствованию, поступающих по каналам обратной связи с руководством.

Следование требованиям стандартов СМИБ предполагает последовательное продвижение к спецификации защитных мер организации (административных, организационных, технологических, технических и иных) и соответствующих целевых процессов деятельности, необходимых для контроля рисков деятельности организации в ее информационной сфере.

В общем случае *этап планирования СМИБ* в соответствии с требованиями стандарта [11] может включать следующие 10 шагов, представленных в таблице 2, реальное наполнение которых определяется самой организацией.

Таблица 2

Шаги при установлении системы менеджмента информационной безопасности

№ п/п	Шаг
1	Определение сферы действия и границ системы менеджмента информационной безопасности в терминах специфики бизнеса, организации, местоположения, активов и технологии, включая подробности о любых исключениях из сферы действия и их обоснование
2	Определение политики системы менеджмента информационной безопасности в терминах специфики бизнеса, организации, местоположения, активов и технологии
3	Определение подхода организации к оценке риска
4	Идентификация рисков
5	Анализ и оценивание рисков
6	Идентификация и оценивание вариантов обработки риска
7	Выбор целей контроля и средств контроля для обработки рисков
8	Получение одобрение руководства по вопросу предлагаемых остаточных рисков
9	Получение санкционирования руководства для реализации и приведения в действие системы менеджмента информационной безопасности
10	Подготовка формулировки применимости требований из каталога требований стандарта

Графически данные шаги иллюстрирует рис. 31.

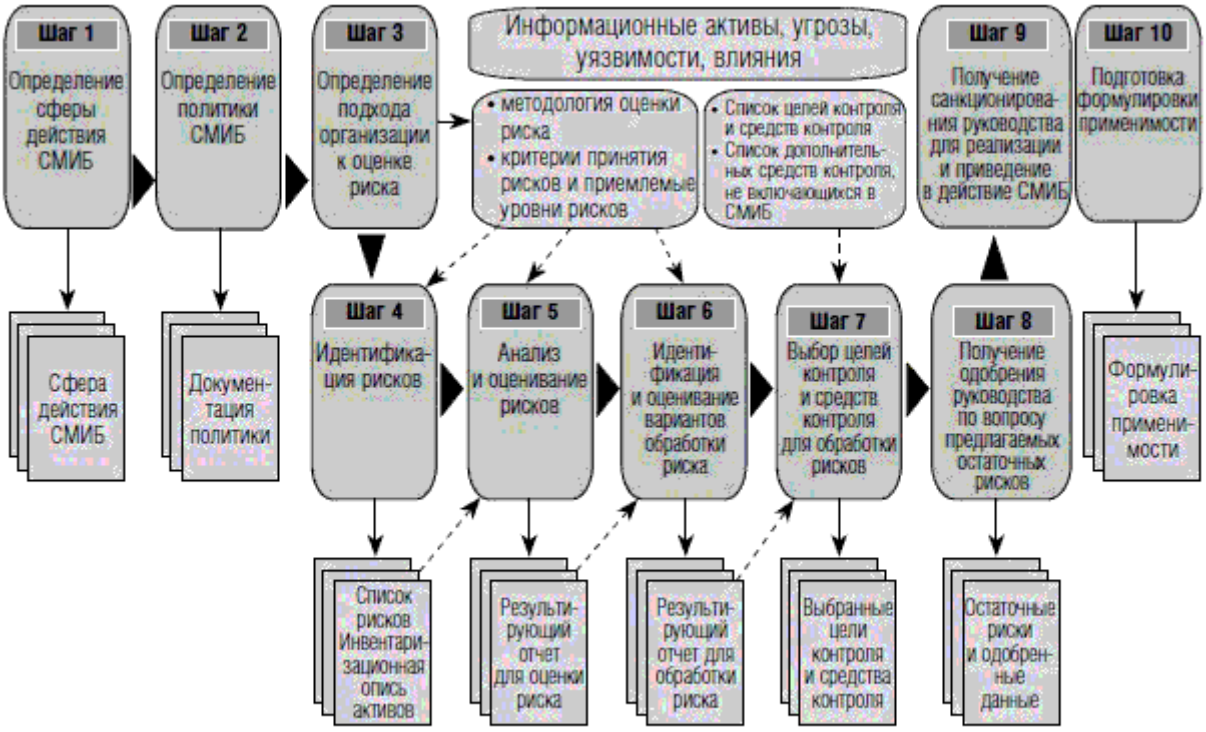


Рис. 31. Шаги при установлении системы менеджмента информационной безопасности

В структуре цикла Деминга результирующие сущности шагов этапа менеджмента «Планирование» иллюстрирует рис. 32.

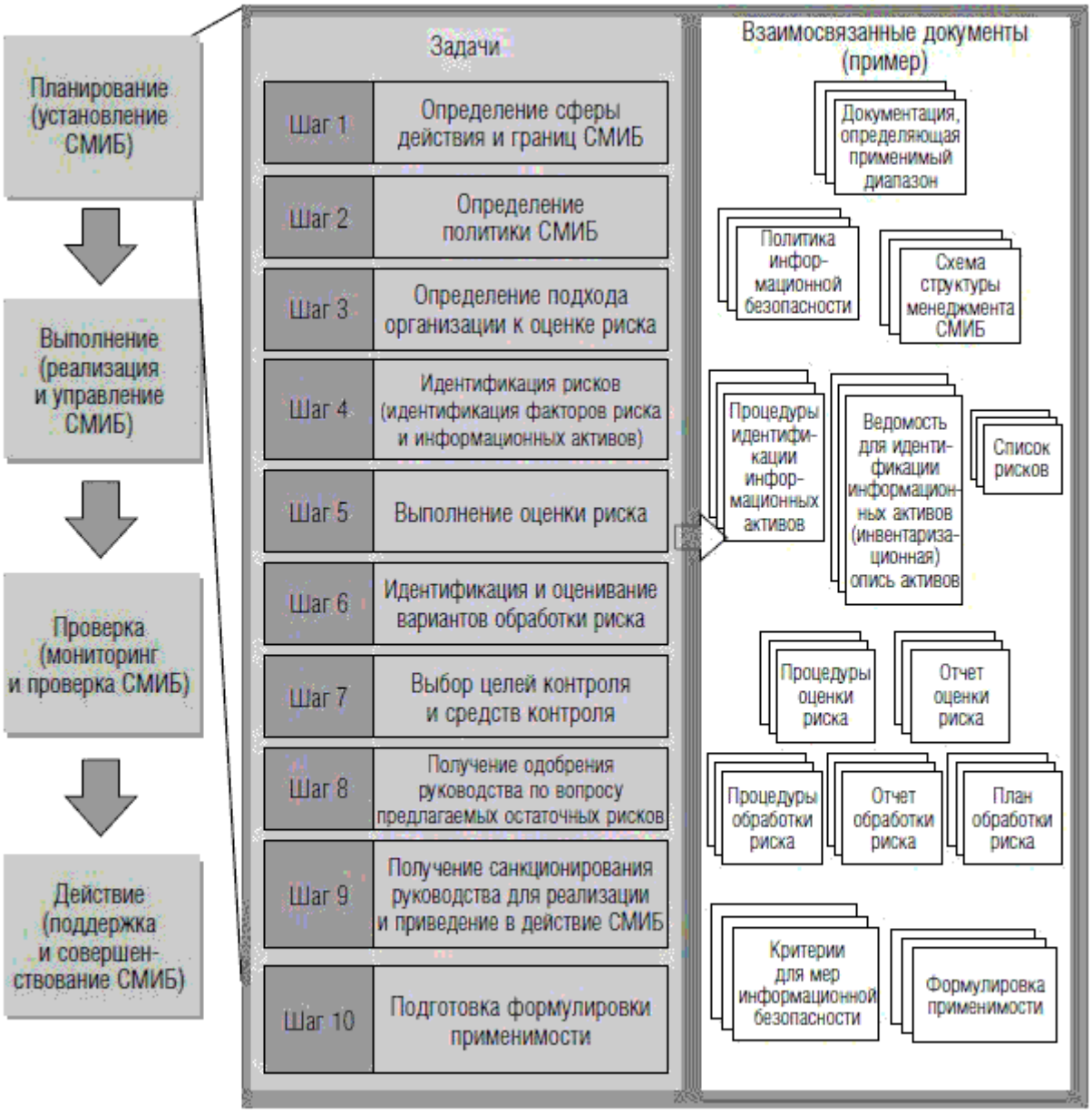


Рис. 32. Шаги для установления системы менеджмента информационной безопасности

Фактически представленные на рис. 31 и 32 шаги этапа планирования СМИБ преследуют цель принятие решения организацией по следующим трем основным вопросам:

– установление сферы применения и политики системы менеджмента информационной безопасности (шаги 1 и 2);

– выбор защитных мер на основе менеджмента риска (шаги 3–7);

– получение одобрения руководства для мер обработки рисков и подготовка формулировки применимости требований из каталога требований стандарта, так как это влечет организационные и, возможно, финансовые издержки компании (шаги 8-10).

При установлении сферы применения и политики системы менеджмента информационной безопасности должны рассматриваться:

– вопроса бизнеса;

– организационные аспекты;

– местоположение (географическое и физическое);

– активы;

– технологии.

Результаты определения применимой сферы действия СМИБ оказывают существенное влияние на объемы работ, которые необходимо будет выполнить при установлении системы менеджмента информационной безопасности. Приведенный ниже рис. 33 показывает общие задачи, связанные с определением применимой сферы действия СМИБ, и сопутствующие элементы.

Политика системы менеджмента информационной безопасности должна закрепить основные концепции менеджмента информационной безопасности в организации. Документы политики (структурно это может включать неограниченное число физически отдельных документов) также могут служить в качестве декларации намерений организации, отражающей то, что организация понимает и несет ответственность за требования информационной безопасности. Это бывает критичным для целей внешнего финансового аудита, если ценные бумаги организации претендуют или представлены на финансовых рынках. Содержание политики системы менеджмента информационной безопасности должно соответствовать политикам бизнеса и принципам и стилю корпоративного управления, устанавливающее основные задачи и цели организации, а также моральные нормы и принципы. Поэтому политики должны формулировать общую базисную точку информационной безопасности и содержать руководства к действию персонала компании, включая операционное руководство (см. рис. 29).

Шаги по установлению политики системы менеджмента информационной безопасности иллюстрирует рис. 34.

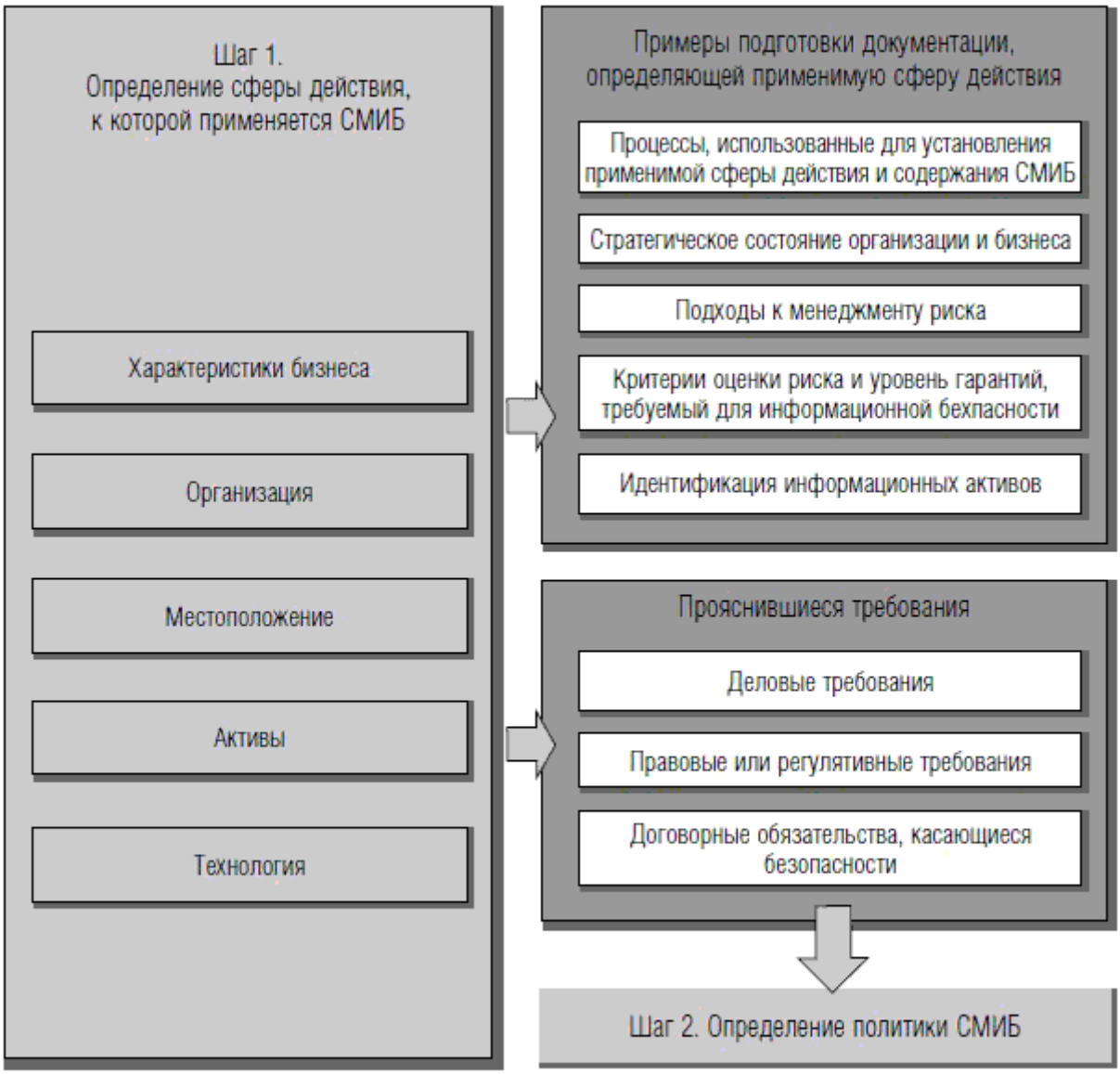


Рис. 33. Определение применимой сферы действия системы менеджмента информационной безопасности

Содержательно вопросы определения политики системы менеджмента информационной безопасности преследуют следующие три основные цели:

– подготовка документов политики системы менеджмента информационной безопасности;

– установление организационной структуры системы менеджмента информационной безопасности;

– получение одобрения руководства (санкционирование работ по модернизации).

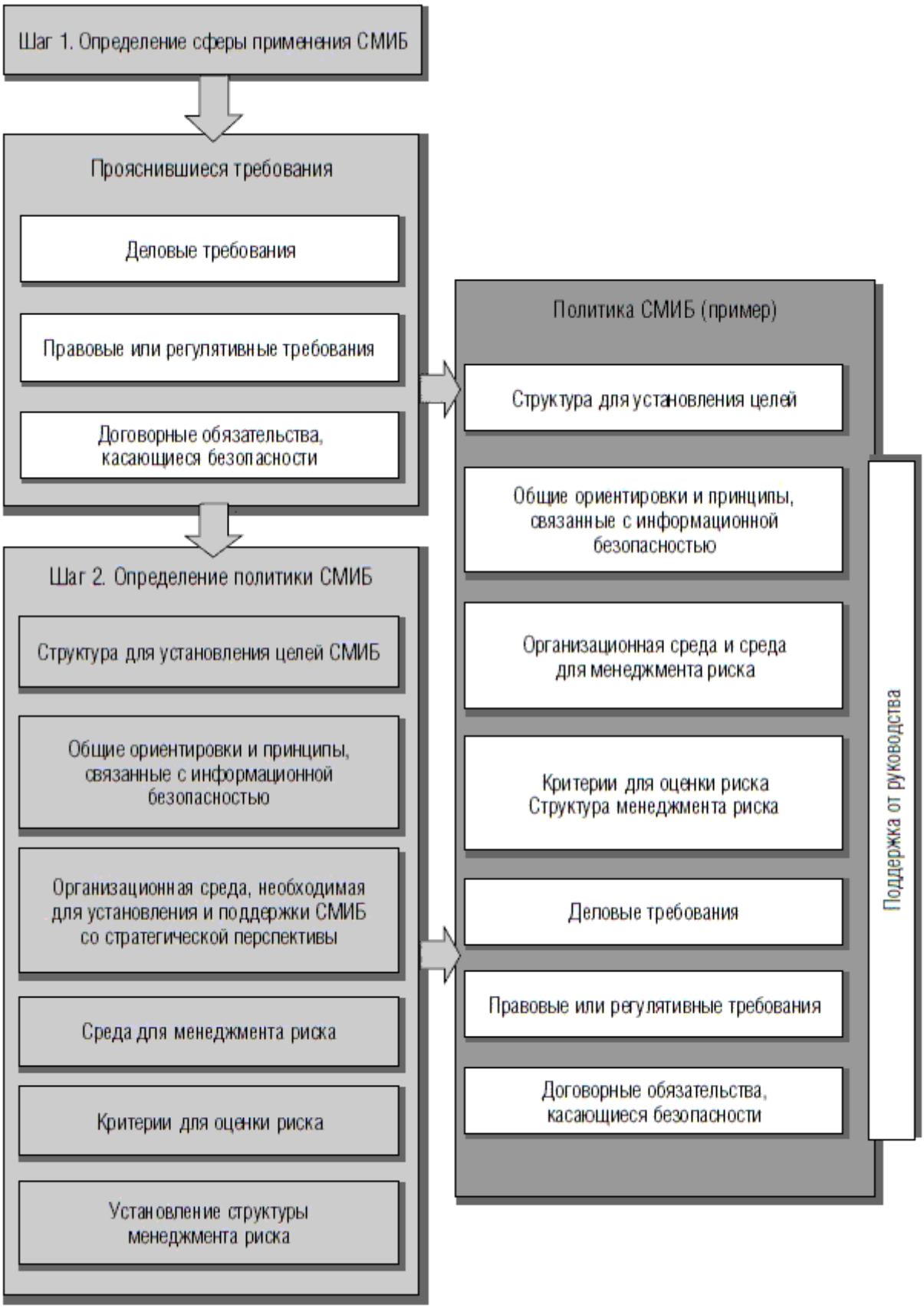


Рис. 34. Шаги для установления политики системы менеджмента информационной безопасности

На основе информации, собранной в «Определении сферы действия системы менеджмента информационной безопасности» и «Установлении политики системы менеджмента информационной безопасности» определяются структуры и цели задач в соответствии с характеристиками организации и требованиями безопасности.

Это формирует основу для принятия решений о подходе к оценке риска. Нижеследующий рис. 35 иллюстрирует основное содержание данного шага работ.

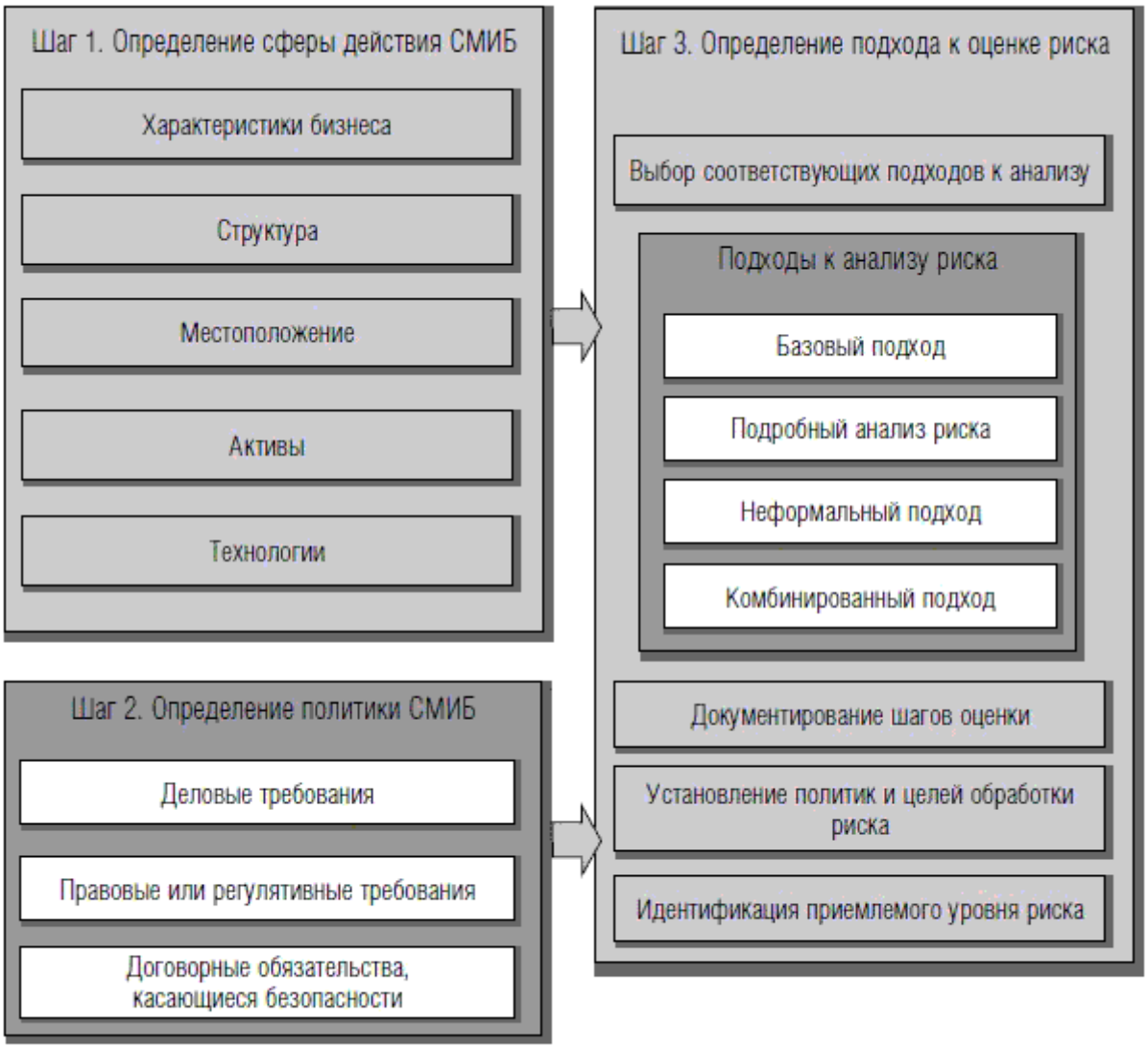


Рис. 35. Определение подхода к оценке риска

В основе методологии стандартной СМИБ лежит риск-ориентированный подход. Он основывается на предположении того, что оценка риска делает возможным понимание следующих вопросов, связанных с информационными активами, которыми владеет организация:

– каковы актуальные угрозы и их источники – факторы риска;

– как часто возможно возникновение угроз;

– сколько и какие информационные активы могут подвергнуться влиянию при возникновении угрозы.

В задаче «Оценка риска» выполняется анализ риска (анализ и прогноз возможных ситуаций, выключая перебор возможных комбинаций: фактор риска, уязвимость актива, негативные последствия) и далее осуществляется соотнесение результатов анализа с некоторым виртуальным уровнем (порогом), что и составляет еще одну операцию – «Оценивание риска».

В науке о безопасности, как правило, выделяется следующие четыре подхода в качестве методов оценки риска.

Базовый подход. Заранее устанавливается определенный уровень безопасности, который должен обеспечиваться, выбираются необходимые для реализации меры и единообразно применяются к каждой рассматриваемой системе.

Неформальный подход. Риски оцениваются на основе имеющегося опыта и суждений специалистов организации или ответственных сотрудников.

Подробный анализ риска. Осуществляется детальная оценка риска путем идентификации и оценивания «ценности активов», «факторов риска», «уязвимостей» и требований безопасности для каждого информационного актива или однородной группы информационных активов.

Комбинированный подход. Используется комбинация вышеперечисленных подходов с целью дополнения недостатков одного подхода преимуществами другого, что должно привести к большей эффективности и точности анализа и оценки.

Любой из указанных подходов в итоге сводится к сравнению с порогом (это самый деликатный и философский объект), что в итоге должно позволить понять, следует ли что-то предпринять или в этом нет необходимости.

Рис. 36 иллюстрирует ситуацию отклонения между реальным измеренным уровнем риска и «требуемым гарантированным уровнем», устанавливаемым организацией для каждого информационного актива. Хотя требуемый гарантированный уровень, показанный на рис. 36, выражен как единый требуемый гарантированный уровень, на практике он может быть неоднородным по своему характеру, а устанавливаться для каждого информационного актива на основе атрибутов и свойств данного информационного актива и его значимости для организации.

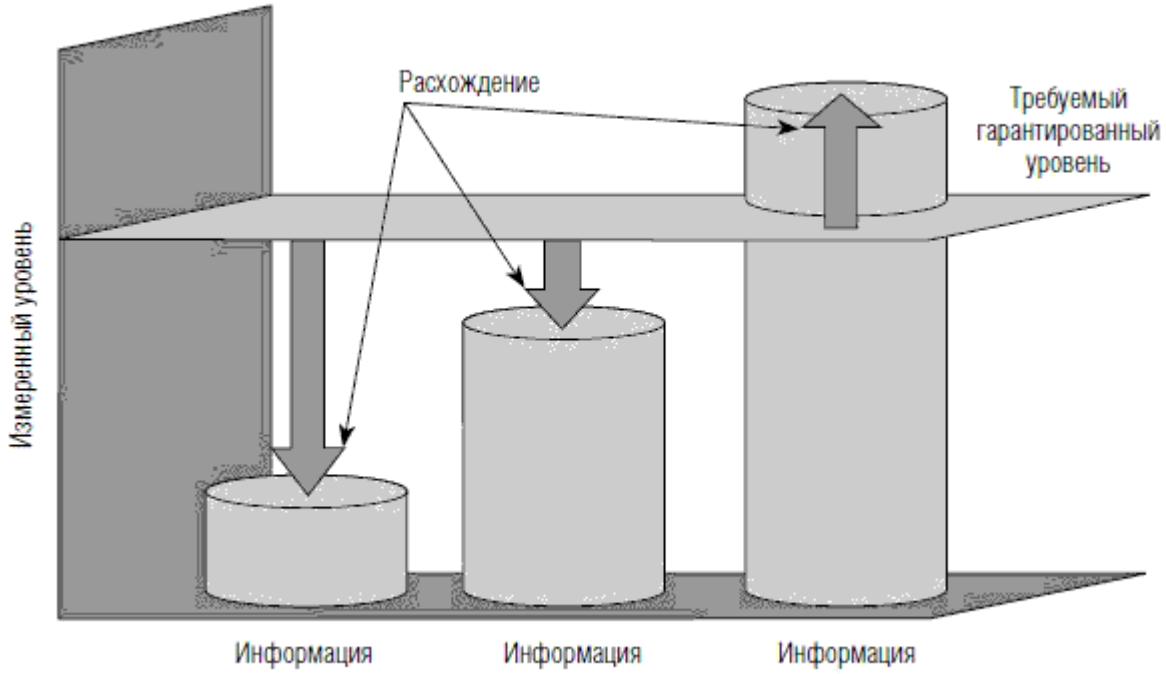


Рис. 36. Требуемый гарантированный уровень

Что касается комбинированного подхода, то он, как правило, сочетает базовый подход с подробным анализом риска, что в итоге признано наиболее эффективной стратегией. Однако определение того, какой подход должен использоваться в определенной ситуации, является нелегкой задачей. Решение о наилучшем подходе зависит от требований безопасности для информационных активов (таких как требования бизнеса, правовые и регулятивные требования и договорные обязательства, касающиеся безопасности, и т. д.).

Целью комбинированного подхода является оценка среды, окружающей каждый информационный актив, и использования соответствующего подхода для анализа риска. Рис. 37 иллюстрирует пример комбинированного подхода.

Оценка риска начинается с идентификации рисков. Однако идентифицируемые риски являются абстрактными, и их трудно понять. Риск формируется из взаимосвязей между несколькими источниками риска. Взаимосвязь между рисками и источниками риска

определяется из «ценности активов», «факторов риска» и «уязвимостей».

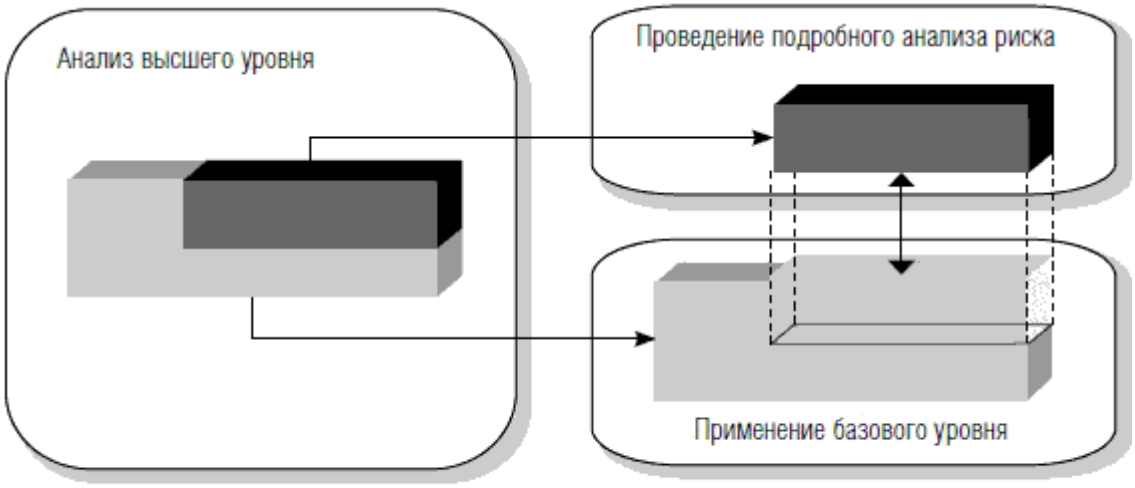


Рис. 37. Комбинированный подход

В процессе идентификации рисков, должны решаться следующие две задачи:
– идентификация информационных активов;
– идентификация факторов риска и уязвимостей.

Идентификация информационных активов включает определение «лиц, отвечающих за информационные активы», подготовку и выполнение инвентаризационной описи активов.

В общем случае в инвентаризационной описи информационных активов должны быть представлены следующие сведения по каждому активу:

– лицо, отвечающее за информацию (владелец или менеджер информационных активов);
– формат информационных активов;
– формат хранения;
– местоположение хранения;
– длительность хранения;
– как следует снимать с эксплуатации активы;
– использование активов;
– масштаб пользователей (и бизнес-процессов);
– зависимости от других процессов.

Отдельная идентификация информационных активов и понимание их свойств будут полезны при идентификации факторов риска и уязвимостей, связанных с последующими задачами, и определении ценности активов. В целом процесс идентификации информационных активов иллюстрирует рис. 38.

«Факторы риска» являются потенциальной причиной инцидентов безопасности, которые могут приводить к потере или повреждению информационных активов организации. Как и в случае определения ценности информационных активов, идентифицируются факторы риска, которые могут оказывать влияние на информационные активы организации. На основе информации о факторах риска, предоставляемой пользователями информации, причастными сторонами из других отделов и внешними специалистами формируется список актуальных угроз и их источников – факторов риска.

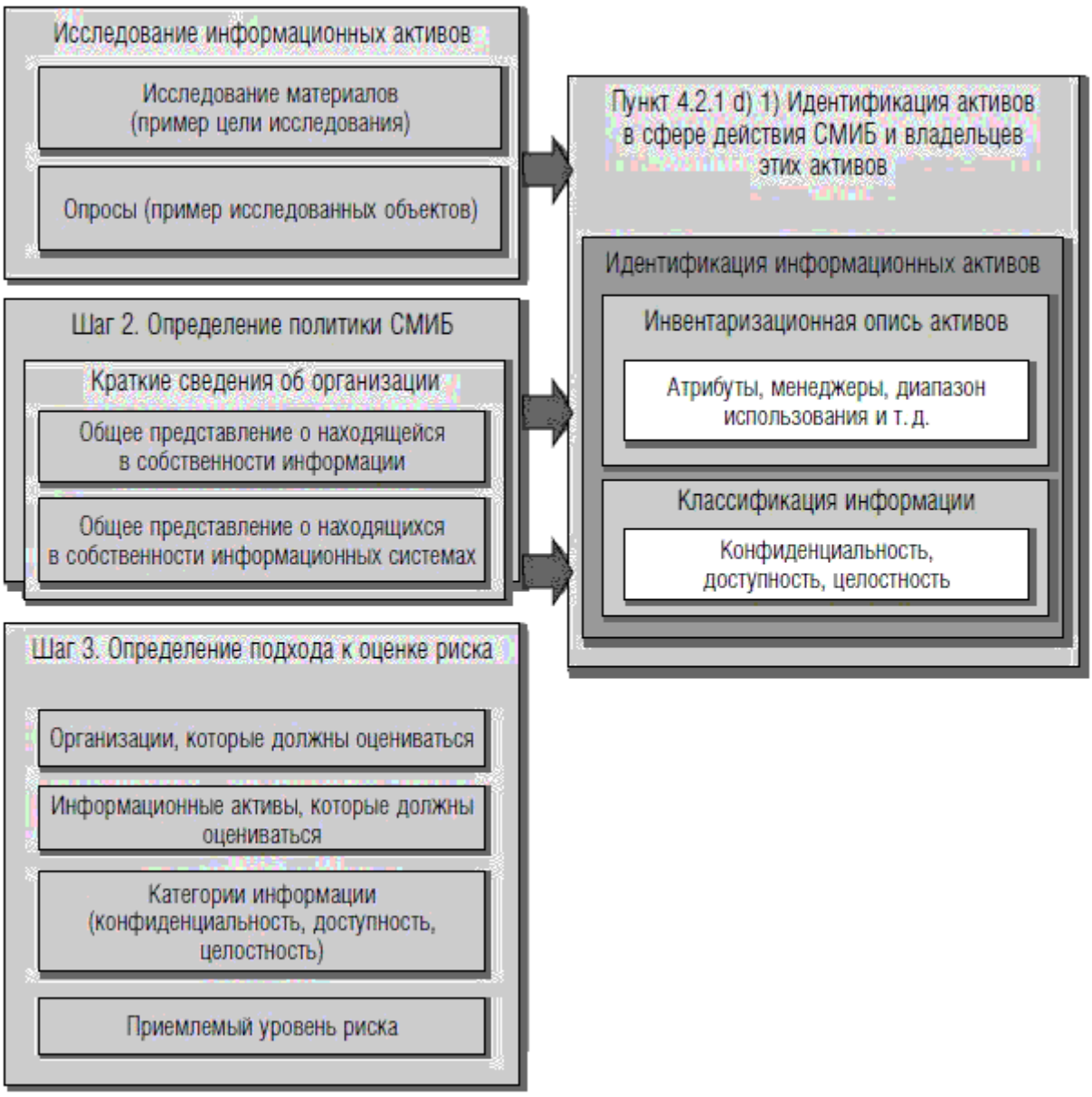


Рис. 38. Идентификация информационных активов

Степень детализации в задачах идентификации информационных активов, факторов риска и уязвимостей определяется выбранным подходом к оценке рисков. Оценка риска может проводиться любым, отвечающим выбранному подходу к оценке рисков методом. Принципиальным здесь является лишь то, что результаты такой оценки должны нас максимально близко подвести к соответствующим типам и видам защитных мер, использование которых предполагается обосновать результатами оценки рисков.

Защитные меры (меры контроля рисков информационной безопасности, рисков бизнеса в информатике), использование которых планируется обосновать результатами оценки рисков, подлежат в последующем отражению в так называемом «Плане обработки рисков». Наряду с предполагаемыми к использованию защитными мерами в плане обработки рисков должны быть зафиксированы стратегии, предполагаемые к реализации организацией в рамках реагирования на выявленные недопустимые риски. Такая стратегия наряду с использованием защитных мер может включать решения по переносу рисков (на клиентов, контрагентов и т. д.), уходу от рисков (прекращение рисковых операций и т. д.) или принятию рисков (ничего не предпринимается).

В случае, если организация в последующем планирует осуществление формального аудита СМИБ или иные подобные шаги, имеющие цель декларирование следования лучшим

практикам и международным стандартам в области обеспечения информационной безопасности, результаты этапа ***«планирование СМИБ»*** должны включать формальный документ «Формулировка (ведомость) применимости». Документ «Формулировка (ведомость) применимости» (оригинальное его наименование Statement of Applicability) имеет преимущественно единственное предназначение: показать, какие требования из каталога мер контроля (защитных мер) стандарта СМИБ реализованы в сфере действия стандартной СМИБ, а какие нет и почему. Потребителями подобных сведений наряду с внешними аудиторами могут быть и лица высшего руководства организации (органа корпоративного управления информационной безопасностью организации, кураторы ИБ). В целом же для практических задач это абсолютно бесполезный документ, который может быть и вредным, если не имеет процедур поддержки его в актуальном состоянии. В этом случае он может ввести в заблуждение лиц высшего руководства организации в случае попытки использования этого документа в своих целях по истечении продолжительного периода времени.

Выработанные на этапе планирования решения должны составить основу основным работам по внедрению/совершенствованию операционной деятельности организации в сфере обеспечения информационной безопасности (естественно, что это касается сферы действия СМИБ). В общем случае это может включать следующие 7 шагов, представленных на рис. 39, выполнение которых уже не предполагает строгую последовательную реализацию, когда последующий шаг не может быть выполнен, так как потребляет (использует) результаты предыдущего (см. шаги этапа ***«Планирование СМИБ»).*** Названия документов, представленных на рис. 39, являются примерными.

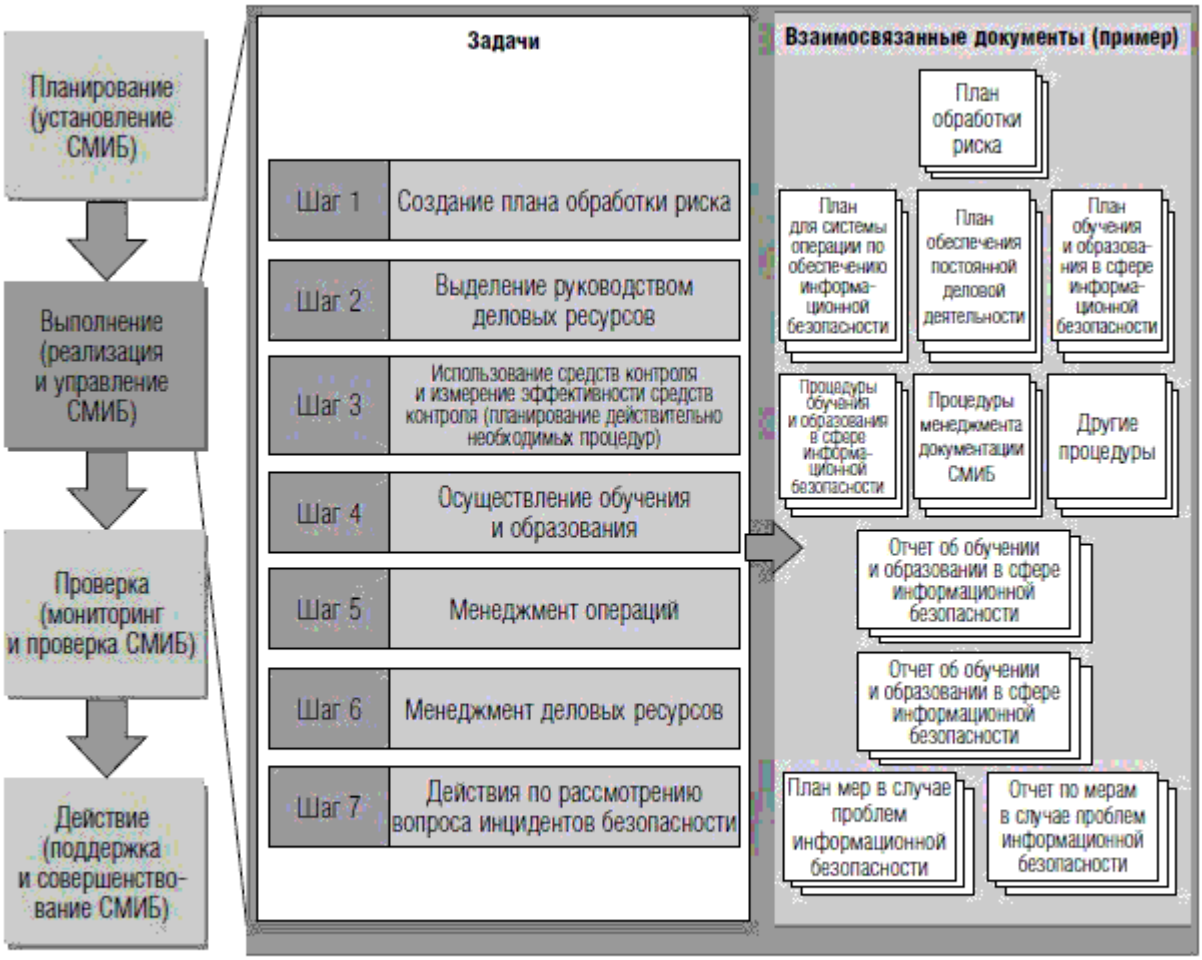


Рис. 39. Процедуры для реализации и управления системой менеджмента информационной безопасности

Отдельные шаги реализации СМИБ могут быть организованы как целевые

(профильные) процессы деятельности, инициируемые и завершаемые по принятым для них критериям (по времени или событию), имеющие собственные самодостаточные регламентирующие нормы в организации, включая организационную и ресурсную поддержку. Это может быть также следствием решений организации в результате реализации требований нескольких стандартизированных систем менеджмента (не только стандартной СМИБ, но и иных стандартизированных менеджментов). Как отмечалось ранее, практически все международные стандарты на системы менеджмента методологически совместимы, что позволяет выделять и поддерживать унифицированные задачи, например, в части работы с персоналом организации, регистрации и сбора индентов и т. п. Процедуры для реализации и управления системой менеджмента информационной безопасности могут быть организованы как система (дерево) процессов (в нотации процессного подхода). При принятии организацией решений о выборе нотации процессного подхода целесообразно обратиться к рекомендациям поддерживающего стандартные требования к СМИБ документа (см. рис. 30): ISO/IEC 27003 «Руководство по реализации СМИБ» [14]. Положения данного международного стандарта основываются на методологии процессного подхода, включая спецификацию всех формальных атрибутов возможных процессов, вытекающих из стандарта требований к СМИБ [11].

Вопросы реализации СМИБ на практике неотделимы от соответствующих процедур контроля, организованных в отдельном блоке требований СМИБ, что часто вводит в заблуждение пользователей стандарта. Шаги задач контроля и проверки иллюстрирует рис. 40. Названия документов, представленных на рис. 40, являются примерными.

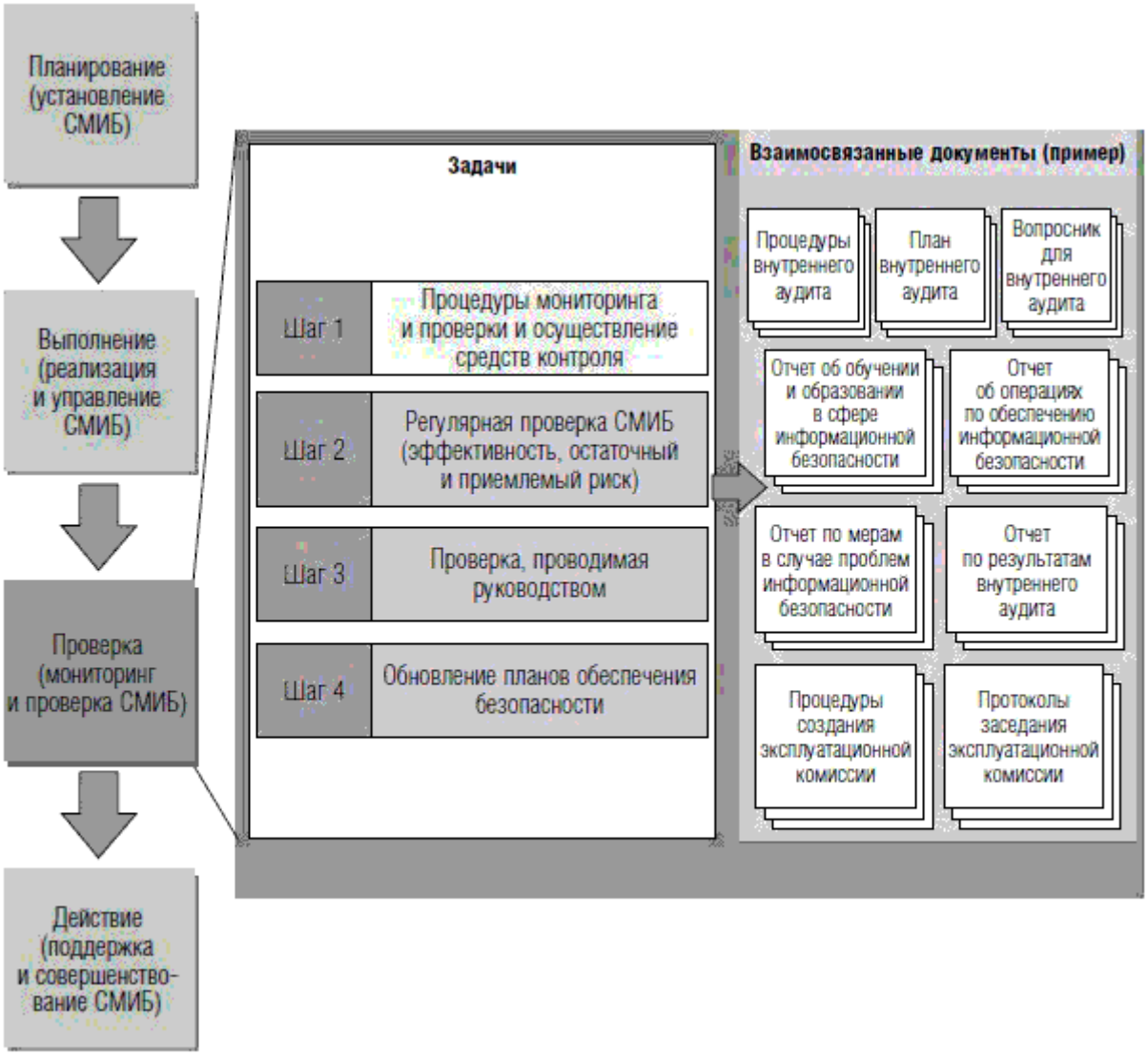


Рис. 40. Процедуры для мониторинга и контроля СМИБ

Формально в содержание работ контроля входят следующие задачи:

– осуществление мониторинга и проверки процедур и других средств контроля рисков (защитных мер) для быстрого обнаружения ошибок в результатах обработки, быстрой идентификации нарушений безопасности и инцидентов, предоставления руководству информации контроля, содействия обнаружению событий безопасности и предотвращения таким образом инцидентом безопасности посредством использования соответствующей системы признаков, определения, были ли эффективными действия, предпринимаемые для ликвидации нарушения безопасности;

– регулярные проверки эффективности СМИБ (включая исполнение политики и целей СМИБ, проверку средств контроля безопасности), учитывая результаты аудитов безопасности, инциденты, результаты измерений эффективности, предложения и мнения от всех заинтересованных сторон;

– пересматривать оценки риска через запланированные интервалы времени, а также остаточные риски и идентифицированные приемлемые уровни риска в соответствии с изменениями вовне организации и в ее операционной и бизнес-среде;

– осуществлять внутренние аудиты СМИБ;

– осуществлять проверки руководством СМИБ для целей подтверждения адекватности сферы действия СМИБ и эффективности мер по совершенствованию СМИБ и т. п.

Все это должно сформировать основу решений по совершенствованию СМИБ. Шаги задач поддержка и совершенствования СМИБ иллюстрирует рис. 41.

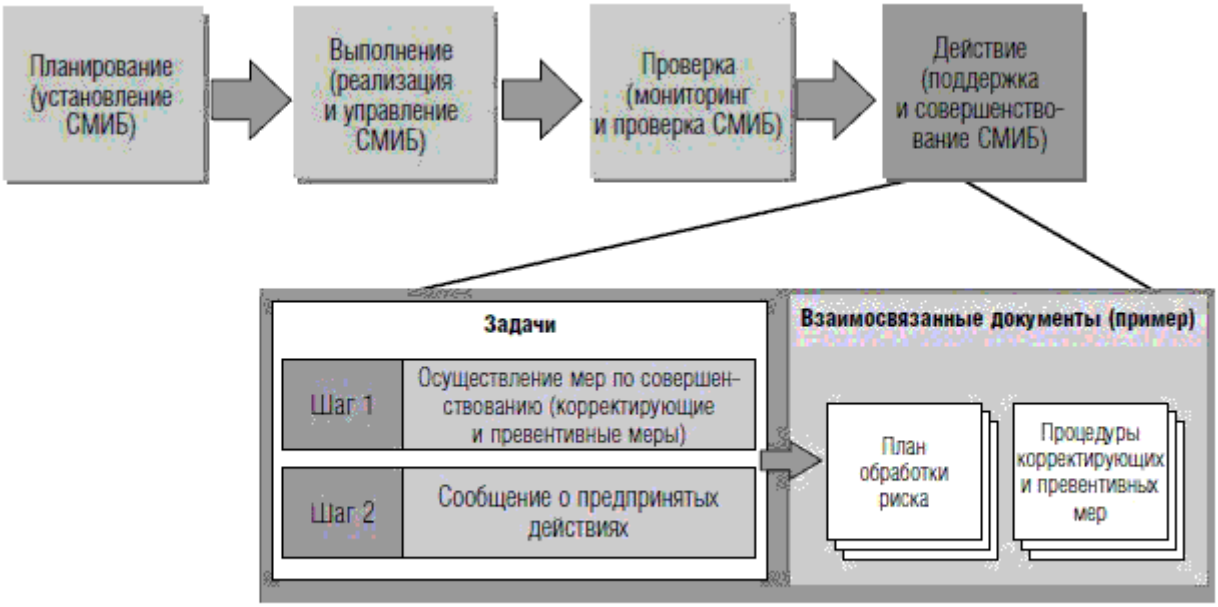


Рис. 41. Поддержка и совершенствование системы менеджмента информационной безопасности

В операционной среде организации требования стандартной СМИБ имеют более сложную конфигурацию, формирующую целевые (профильные) виды деятельности, требующие своего менеджмента (обозначим как «частный менеджмент»). Рис. 42 иллюстрирует возможный состав таких частных менеджментов, поддерживаемых задачи СМИБ.

Рис. 42. Структура частных менеджментов СМИБ

В то же время информационные потоки в среде организации (операций и функций управления) могут содержать критерии, требующие реализации согласованных действий, формально относящихся к различным видам деятельности в организации (различным частным менеджментам). Рис. 43 иллюстрирует работу событийной модели текущей деятельности, порожденной выявленным событием ИБ (от блока «Процессы мониторинга»).

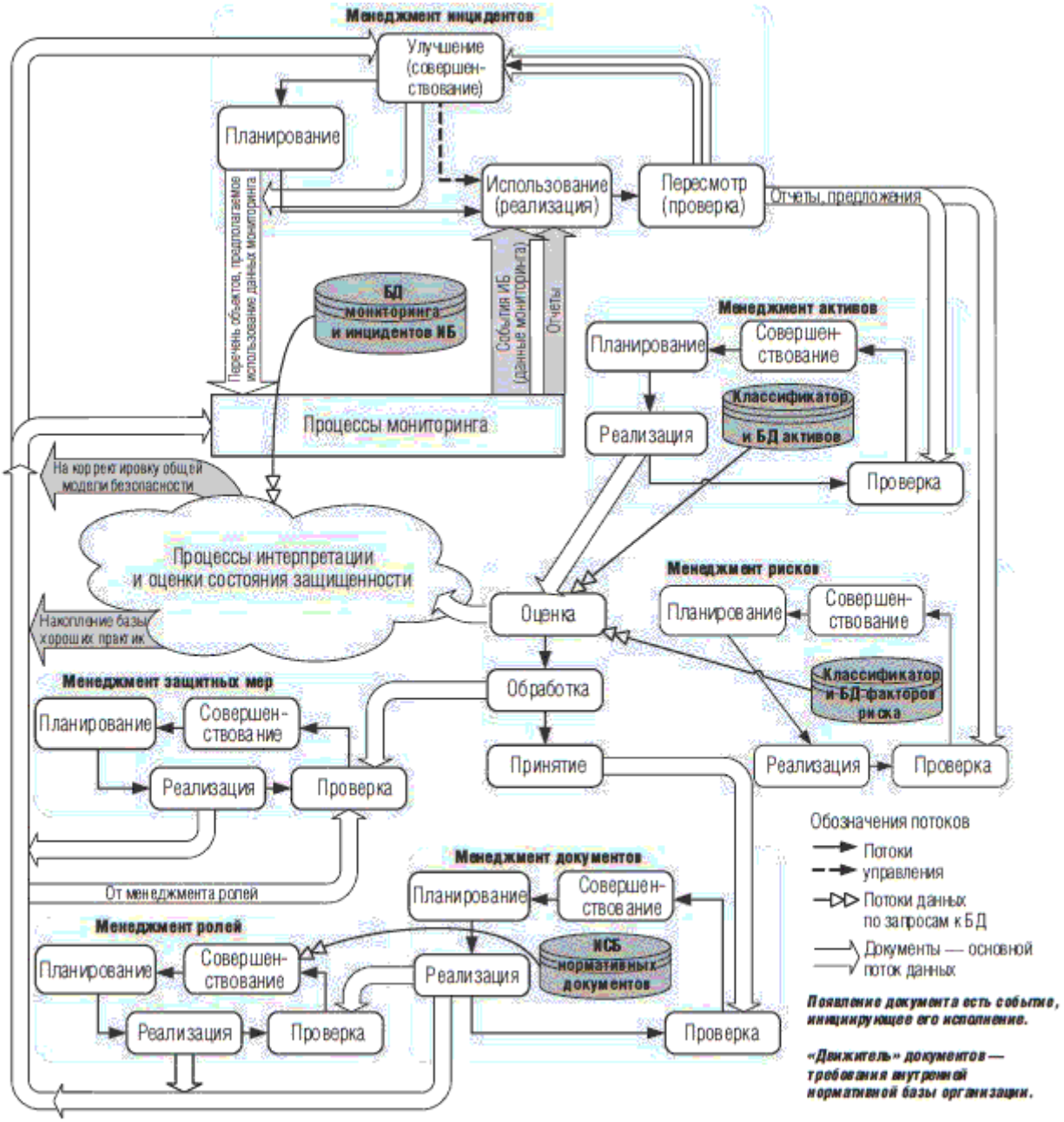


Рис. 43. Иллюстрация функционирования событийной модели Деминга — Шухарта на частных менеджментах

Далее более подробно рассмотрим вариант (пример) взаимодействия различных видов деятельности в организации (совместную работу «частных менеджментов» СМИБ) на примере процессов мониторинга и обработки инцидентов информационной безопасности.

2.2.4. Реализация моделей менеджмента в целевых задачах организации («частные менеджменты»)

При рассмотрении примера будем исходить из взаимосвязанной деятельности по менеджменту инцидентов и мониторингу, показанной на рис. 44. При этом процессы цикла Деминга – Шухарта применительно к менеджменту инцидентов называются в соответствии с международным документом [15].

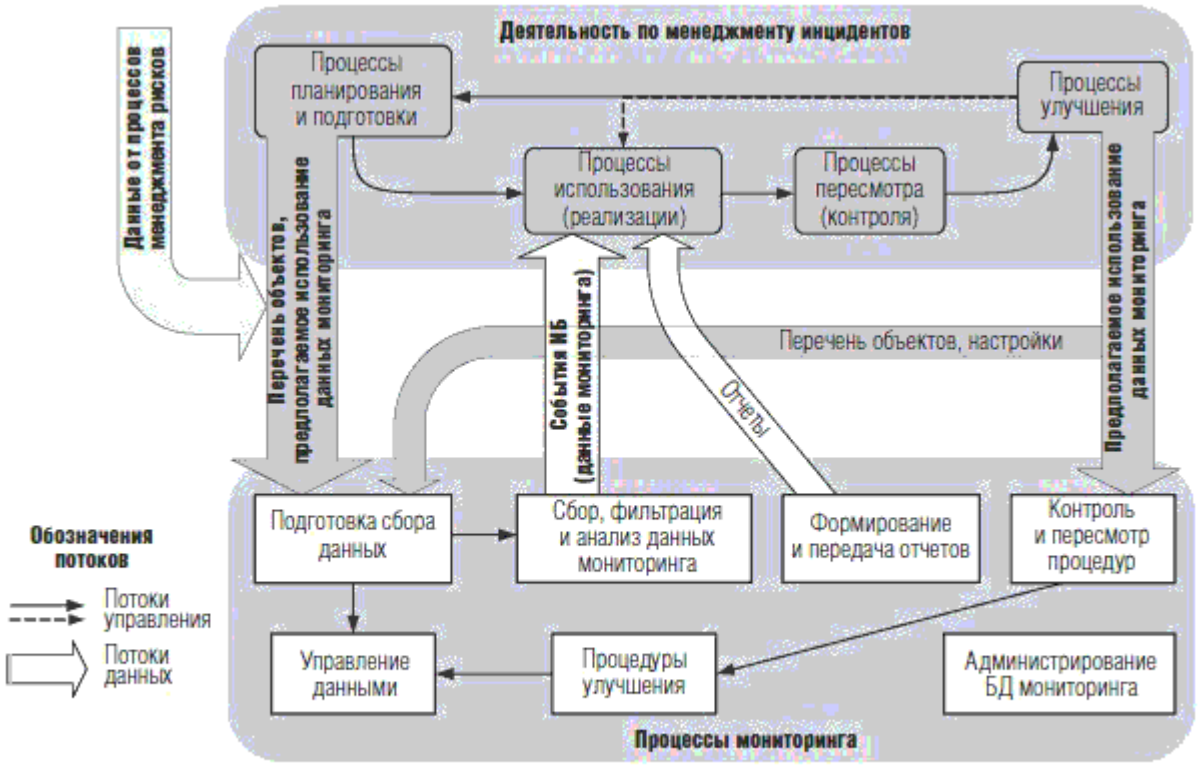


Рис. 44. Взаимосвязь деятельности по менеджменту инцидентов и мониторингу

В процессе реагирования на инцидент ИБ в соответствии с документом [15] предусматриваются процедуры пересмотра и улучшения процессов менеджмента инцидентов ИБ как на регулярной основе (периодически), так и по результатам обработки любого существенного инцидента ИБ. Завершающий отчет по каждому инциденту ИБ сохраняется в базе данных инцидентов ИБ (см. рис. 44, 43) и включает данные, которые могут быть использованы в будущем при обработке подобных инцидентов, включая их предвестники и признаки.

Предложения по улучшению должны отражать вопросы о дополнительном инструментарии или ресурсах, обучении персонала и т. п., т. е. все, что необходимо для принятия решений, направленных на выбор и реализацию мер по совершенствованию:

– менеджмента инцидентов ИБ;

– оценки рисков ИБ;

– инициирования улучшений безопасности, обновления и (или) реализации новых защитных мер ИБ и в итоге совершенствования СМИБ.

Документы, выпускаемые в процессе менеджмента инцидентов, фактически являются событиями, инициирующими процессы в других частных менеджментах, поскольку служат источниками сигнала для инициирования иных работы. Например, в процессе менеджмента информационных активов будет определена структура активов, их ценность, важность, приоритеты свойств безопасности, уязвимости и другие свойства. Однако большая часть этих свойств определяется экспертным путем или получается в результате опроса, т. е. может носить неточный или субъективный характер. Один из путей проверки объективности этих данных – использование фактического материала, сопровождающего факты инцидентов или содержащегося в периодических аналитических отчетах. Документы, появляющиеся в процессе менеджмента инцидентов, являются входными для процесса ***проверки*** при менеджменте активов (см. рис. 43, поток от процесса ***«Пересмотр»*** в менеджменте инцидентов к процессу ***«Проверка»*** в менеджменте активов). При ***проверке*** будет выяснено, какая конкретно уязвимость была использована в инциденте, какие еще информационные активы были затронуты, были ли предвестники, насколько быстро удалось

выделить все признаки инцидента и понять, как его сдерживать, каков ущерб в результате произошедшего инцидента, насколько быстро восстановлена функциональность, связанная с активом, и т. п. Эти данные позволят скорректировать (процесс ***«Совершенствование»)*** свойства вовлеченных в инцидент активов и, возможно, их структуру, реальную ценность и важность.

По результатам менеджмента инцидентов корректируются также и перечень факторов риска, менеджмент которых на рис. 43 включен в менеджмент риска. Однако изменение актуальности факторов риска или появление новых источников рисков, методов атак и т. п. должно приводить к переоценке риска.

Изменение защитных мер, регламентов и ролей неизбежно отражается на менеджменте инцидентов. Таким образом, цикл замкнулся. Если, к примеру, в процессе «***Пересмотр*** » менеджмента инцидентов появилась рекомендация о включении дополнительного параметра мониторинга на сервере системы, то этот вопрос, скорее всего, нельзя решить в рамках менеджмента инцидентов.

Описанная событийная схема инвариантна к организационной структуре операционной среды. Она отражает основной смысл «процессного подхода» – ориентацию на результат. В практике наибольшую сложность вызывает вопрос отображения необходимых работ на должностные обязанности персонала. Например, совсем не обязательно, чтобы менеджмент защитных мер осуществлялся в рамках деятельности службы информационной безопасности компании. Более того, он может быть разнесен по нескольким подразделениям службы информатизации в соответствии с функционалом этих защитных мер (антивирусная защита, телекоммуникации, серверное хозяйство и т. п.).

На практике организационная составляющая обеспечения информационной безопасности бизнеса чрезвычайно разнообразна. Профильные структуры и подразделения, за которыми формально закреплены обязанности по обеспечению информационной безопасности бизнеса, могут быть организованы как:

– самостоятельное подразделение в структуре службы безопасности организации;
– отдел в подразделении экономической безопасности;
– отдел в структуре службы информатизации банка;
– отдельная группа в составе подразделения риск-менеджмента компании.

Последний вариант не гипотетический, а совершенно реальный, и не экзотический, а достаточно распространенный и имеющий свои уникальные сильные и слабые стороны. Обусловлен он, как правило, ситуацией, когда служба безопасности организации комплектуется только отставными офицерами силовых ведомств, которые прекрасно владеют навыками и приемами решения «классических» задач безопасности (физическая защита, видео/аудио и т. п.), но имеют сложности в обращении со средствами и системами вычислительной техники, составляющими в настоящее время значимую часть информационной сферы компаний.

В этих условиях руководство организации вынуждено рассматривать альтернативные варианты размещения в операционной среде компании «функции обеспечения информационной безопасности», исходя из собственного понимания возможного вклада и содействия этой функции результатам деятельности организации.

С точки зрения бизнеса и высшего руководства организации процедуры, меры и средства обеспечения информационной безопасности деятельности в конечном итоге предназначены для контроля рисков бизнеса (деятельности) организации, проистекающих от факторов рисков в информационной сфере. При таком видении вопроса принципиальной важности не составляет вопрос о том, где учредить орган ответственности за «функцию обеспечения информационной безопасности», значимым является в итоге лишь то, чтобы эта функция работала, как ожидается, и приносила пользу организации.

Более того, «функция обеспечения информационной безопасности» в современных условиях во многих организациях, в особенности в так называемых «развитых странах»,

понимается как интегрирующая платформа всех средств контроля информационных технологий и иных видов деятельности в организации (см. рис. 26). Обеспечение информационной безопасности относится и к инфраструктуре, и к данным и формирует основу эффективности, за редким исключением, большинства иных используемых в организации средств системы внутреннего контроля, представляя ей необходимую документальную фактуру по реальным событиям в операционной среде организации. Исключение, например, могут составлять средства контроля, связанные с финансовыми аспектами ИТ (например, средства контроля рентабельности инвестиций, средства контроля бюджета обслуживания и поддержки стоимости владения), некоторые средства контроля управления проектами внедрения средств и систем автоматизации и информатизации деятельности организации.

Это нашло свое отражение и в международных стандартах менеджмента и обеспечения информационной безопасности, формируя некие единый язык общения различных подразделений организации, следующих таким стандартам. Данное обстоятельство не в последнюю очередь послужило росту популярности на стыке XX и XXI вв. британского стандарта BS 7799 «Системы менеджмента информационной безопасности». В его положениях, возможно, впервые в международной практике был предложен понятийный аппарат области информационной безопасности, где «традиционные» средства и меры защиты и обеспечения информационной безопасности были обозначены как «меры контроля [рисков]» деятельности организации.

В последних редакциях действующих международных стандартов и во вновь принимаемых документах на уровне определения базовых понятий были объединены и рассматриваются в качестве синонимов такие понятия, как «контроль» и «защитная мера». Например, ГОСТ Р ИСО/МЭК 13335-1-2006 [17] (гармонизированный международный стандарт) вводит следующие понятия:

«2.7 контроль (control): – [нет определения понятия]

Примечание – В контексте безопасности информационно-телекоммуникационных технологий термин «контроль» может считаться синонимом «защитной меры» (см. 2.24).

2.24 защитная мера (safeguard): Сложившаяся практика, процедура или механизм обработки риска.

Примечание – Следует заметить, что понятие «защитная мера» может считаться синонимом понятию «контроль» (см. 2.7)».

Другой международный стандарт ISO/IEC 27002 [18], включающий структурированный каталог защитных мер для использования в системах менеджмента информационной безопасности, предлагает следующее понятие, характеризующее то, что включает и устоявшееся понятие «защитная мера»:

«Мера контроля (control) – средство менеджмента риска, включающее в себя политики, процедуры, рекомендации, инструкции или организационные структуры, которые могут иметь административную, техническую, управленческую или правовую сущность.

Примечание – Термин «мера контроля» может использоваться также в качестве синонима к терминам «защитная мера» (safeguard) или контрмера (countermeasure)».

При этом в положениях ISO/IEC 27002 [18] отмечается, что следующие меры контроля рассматриваются как общепринятая практика в области информационной безопасности («джентльменский набор» для «публичных» компаний):

а) наличие документа, описывающего политику информационной безопасности;

б) распределение обязанностей по обеспечению информационной безопасности;

в) обеспечение осведомленности, образования и обучения вопросам информационной безопасности;

г) правильная обработка данных в приложениях;

д) менеджмент технических уязвимостей;

е) менеджмент непрерывности бизнеса;

ж) менеджмент инцидентов, связанных с информационной безопасностью, и действий по улучшению реагирования на них.

Даже перечисленные категории защитных мер («мер контроля и управления рисками» в терминах современных стандартов), несмотря на их скромную номенклатуру, серьезным образом влияют на всю операционную среду организации. При этом основным их назначением является формирование оснований для уверенности высшего руководства (собственников бизнеса) в надежности (адекватности, устойчивости, безопасности и т. д.) операционной среды организации, касающееся ее информационной составляющей. Те же цели в своей деятельности преследует и система (подразделение) внутреннего контроля организации, и система (подразделение) менеджмента рисков организации. Все это приводит к необходимости четкого позиционирования и понимания потенциального вклада перечисленных направлений деятельности подразделений организации в формирование единой системы мер гарантий и уверенности в достижении заявленных целей. Это предполагает также и противодействие на всех уровнях неправомерным (преднамеренным и /или случайным) действиям сотрудников компаний и внешних лиц, способных привести к негативным последствиям как для организации, так и для ее клиентов, инвесторов и т. п. Методам и мерам контроля рисков деятельности для организации в целом, а также процессам деятельности в сфере информатизации организации посвящены модельные решения, нашедшие отражение в ряде авторитетных источников, например, таких, которые известны как COSO, COBIT, ITIL.

2.3. Модели COSO, COBIT, ITIL

Структура, получившая широкую известность под аббревиатурой COSO (The Committee of Sponsoring Organizations [of the Treadway Commission] – Комитет спонсорских организаций [комиссии Тредвея]), была учреждена в 1985 г. COSO был создан для финансирования работ независимой национальной (американской) комиссии, образованной для выработки мер противодействия мошенничеству с финансовой отчетностью. Целью деятельности комиссии являлось изучение факторов, которые могут приводить к мошенничеству с финансовой отчетностью, а также выработка рекомендаций для частных компаний и их независимых аудиторов, для инспекторов Комиссии США по ценным бумагам и биржевым операциям (SEC) и других инспекторов и образовательных учреждений.

Спонсорами (членами COSO) выступили профессиональные организации (ассоциации), которые напрямую зависели от последствий фактов мошенничества с финансовой отчетностью. Это пять профессиональных ассоциаций, располагавшихся в США: Американская ассоциация бухгалтеров, Американский институт дипломированных общественных бухгалтеров, Международная ассоциация финансовых руководителей, Институт внутренних аудиторов и Национальная ассоциацией бухгалтеров (ныне известен как Институт бухгалтеров-управленцев). Комиссию возглавили шесть инспекторов во главе с Джеймсом Тредвеем-младшим, на то время бывшим уполномоченным Комиссии по ценным бумагам и биржевым операциям США. В комиссию вошли представители промышленности, независимого бухгалтерского учета и аудита, инвестиционных компаний и Нью-Йоркской фондовой биржи.

Результаты не заставили себя долго ждать. В октябре 1987 г. после годичного обсуждения был опубликован первый отчет Комиссии, рассматривающий следующие вопросы:

– обзор систем финансовой отчетности и мошенничество в финансовой отчетности;

– рекомендации для публичных (акционерных) компаний;
– рекомендации для независимых аудиторов;
– рекомендации Комиссии по ценным бумагам и биржевым операциям и другим органам, вовлеченным в регулирование данной области деятельности;
– рекомендации для образовательных задач;
– приложения (аналитика, практические примеры).

Фактически первый отчет комиссии 1987 г. дал направленность всем последующим публикациям, известным под аббревиатурой COSO. К настоящему времени основные направления деятельности комиссии отражены в документах, посвященных следующим вопросам:
– анализ фактов мошенничества в финансовой отчетности;
– внутренний контроль;
– менеджмент риска в организации.

Документы комиссии по вопросам организации внутреннего контроля и риск-менеджмента в компаниях наиболее востребованы практикой в сфере корпоративного управления и контроля (аудита). Процессы глобализации финансовых, сырьевых, товарных рынков послужили дополнительным стимулом поиска универсальных методологических (модельных) платформ функционирования организаций (моделей деятельности организаций). Модель системы внутреннего контроля COSO уже де-факто стала эталоном организации внутрикорпоративной деятельности. Более десяти лет назад Комиссия COSO выпустила один из первых документов «Концептуальные основы внутреннего контроля», направленный на оказание помощи предприятиям и организациям в проведении оценки и совершенствовании их систем внутреннего контроля. Тысячи компаний приняли и использовали эту концепцию при выработке решений относительно своих политик, правил и процедур внутреннего контроля.

В 2001 г. COSO инициировал проект по разработке концептуальных основ менеджмента риска для использования руководством компаний при оценке своей системы управления рисками и ее дальнейшем совершенствовании. Период разработки концептуальной базы по менеджменту риска COSO был отмечен рядом корпоративных скандалов и банкротств в Европе и Америке, получивших широкую огласку и принесших значительные убытки инвесторам, персоналу компаний и другим заинтересованным сторонам. В этих условиях потребность в создании концептуальной базы по менеджменту рисками, устанавливающей основные принципы и концепции, общую терминологию, четкие указания и рекомендации, стала еще более очевидной.

Одним из последствий указанных событий стало принятие в 2002 г. в США так называемого Закона Сарбейнса – Оксли (известного как SOX). Аналогичные законы были приняты или готовятся к принятию и в других странах. Указанная серия законов расширяет существовавшие требования к открытым акционерным обществам по созданию и поддержанию систем внутреннего контроля, возлагая обязанность на руководство компаний представлять информацию об эффективности таких систем, а на независимого аудитора [финансовой отчетности] – удостоверять предоставленные сведения.

Одним из самых важных вопросов, решаемых высшим руководством организаций, как отмечается в материалах COSO, является определение величины риска, который организация готова принять и принимает в процессе своей деятельности по созданию добавленной стоимости (материалы комиссии, финансируемой COSO, обращены к коммерческим структурам, в связи с этим в ее материалах делается акцент на прибыль/добавленную стоимость).

Основная предпосылка при менеджменте рисками деятельности организации заключается в том, что каждая организация существует, чтобы создавать добавленную стоимость для сторон, заинтересованных в ее деятельности. При этом все организации

сталкиваются с неопределенностью, и задачей руководства является принятие решения об уровне неопределенности, с которым организация готова смириться, стремясь увеличить стоимость для заинтересованных сторон. В связи с этим неопределенность, с одной стороны, таит в себе риск (потери), а с другой – может открыть новые возможности, поэтому принятые в условиях неопределенности решения могут привести как к снижению, так и к увеличению стоимости. Менеджмент риска, как отмечается в материалах COSO, позволяет руководству эффективно действовать в условиях неопределенности и связанных с ней рисков и использовать возможности, увеличивая потенциал для роста стоимости компании.

Рост стоимости будет максимальным, если руководство определяет стратегию и цели таким образом, чтобы обеспечить оптимальный баланс между ростом компании, ее прибыльностью и рисками; эффективно и результативно использует ресурсы, необходимые для достижения целей организации.

В соответствии с методологией COSO менеджмент риска организации включает в себя следующие ключевые задачи:

– определение уровня риска, на который готова идти организация в соответствии со своей стратегией развития;

– совершенствование процесса принятия решений по реагированию на возникающие риски;

– сокращение числа непредвиденных событий и убытков в хозяйственной деятельности;

– определение и управление всей совокупностью рисков в хозяйственной деятельности;

– использование благоприятных возможностей;

– рациональное использование капитала.

Возможные подходы к определению уровня риска, на который готова идти организация (величину приемлемой степени риска), схематично иллюстрирует рис. 45.

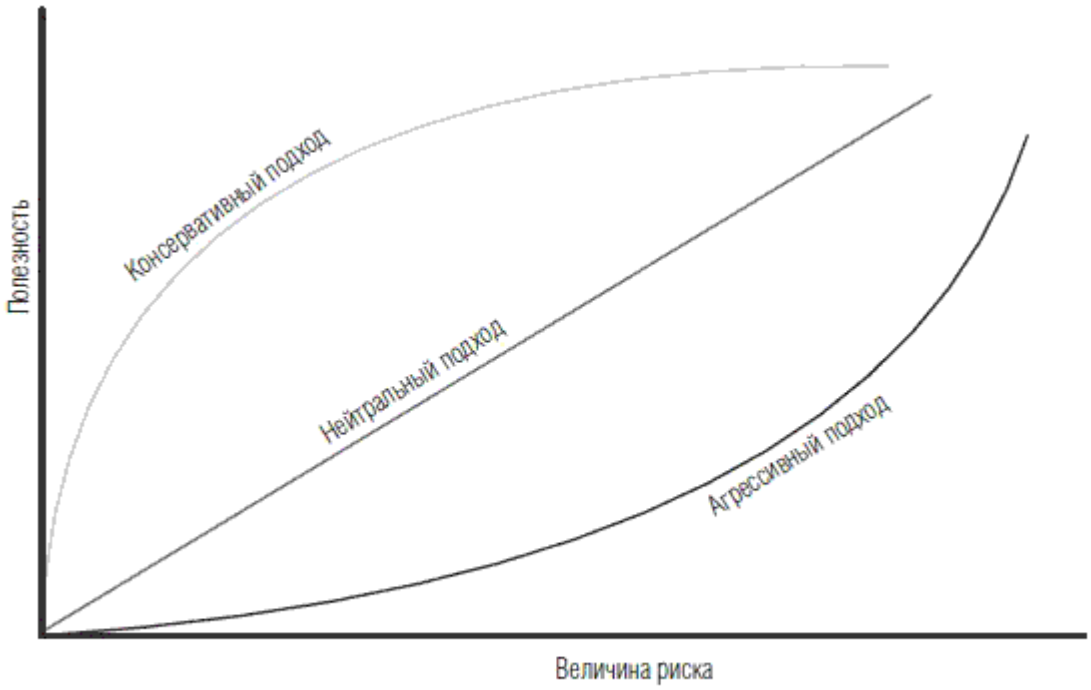


Рис. 45. Подходы к определению величины приемлемой степени риска

По мнению авторов рекомендаций COSO, возможности, открываемые процессом менеджмента риска организации, помогают руководству в достижении целевых показателей прибыльности и рентабельности, а также в предотвращении нерационального использования ресурсов. При этом процесс менеджмента риска способствует обеспечению эффективности процесса составления финансовой отчетности, а также соблюдения законодательных и

нормативных актов, избежания нанесения ущерба репутации компании и связанных с этим последствий. Посредством этого процесс менеджмента риска позволяет руководству достигать своих целей и при этом избегать просчетов и неожиданностей.

Влияние событий в сфере неопределенности может быть положительным, отрицательным или одновременно и тем и другим. События, влияние которых является отрицательным, методологией COSO предлагается относить к риску, который мешает созданию или ведет к снижению стоимости. События, влияние которых является положительным, могут компенсировать отрицательное влияние рисков, а также положительно влиять на достижение результата.

По COSO менеджмент риска организации:

– представляет собой непрерывный процесс, охватывающий всю организацию;

– осуществляется сотрудниками на всех уровнях организации;

– используется при разработке и формировании стратегии;

– применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации;

– нацелен на определение событий, которые могут влиять на организацию и менеджмент рисками таким образом, чтобы они не превышали порог готовности организации идти на риск;

– дает руководству и совету директоров организации разумную гарантию достижения целей;

– связан с достижением целей по одной или нескольким пересекающимся категориям.

Существует прямая взаимосвязь между целями, или тем, чего организация стремится достичь, и компонентами процесса менеджмента рисками организации, представляющими собой действия, необходимые для их достижения. Данная взаимосвязь иллюстрируется в материалах COSO трехмерной матрицей (кубом), представленным на рис. 46.

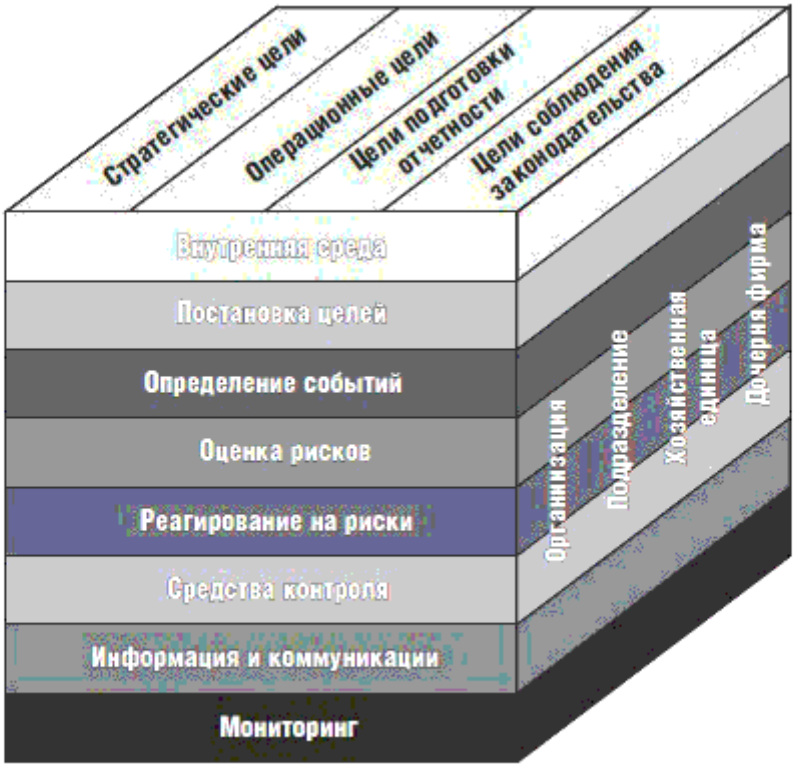


Рис. 46. Связь между целями организации и компонентами процесса менеджмента риска организации

Данный рисунок отражает пересмотренный подход руководств Комитета COSO (называемые еще COSO II), которые являются более детализированным по сравнению с материалами, лежащими в основе первого блока руководств Комитета COSO, датируемого

началом 1990-х гг.

Применение систематизированного подхода в рамках менеджмента риска организации позволяет обеспечить оптимальное управление ситуацией в условиях неопределенности и принятие более осознанных решений по вопросам риска. Для реализации данного подхода на практике организация должна разработать/принять удовлетворяющую ее целям понятийную базу, установить цели, задачи, объемы, распределить ответственность, а также утвердить методологию управления операционными рисками.

Восемь взаимосвязанных компонентов менеджмента риска организации по методологии Комитета COSO (см. рис. 46) поясняются следующим образом.

– Внутренняя среда. Внутренняя среда представляет собой атмосферу в организации и определяет, каким образом риск воспринимается сотрудниками организации и как они на него реагируют. Внутренняя среда включает философию менеджмента риска и уровень риска, на который готова идти организация, честность и этические ценности, а также ту среду, в которой они существуют.

– Постановка целей. Цели должны быть определены до того, как руководство начнет выявлять события, которые потенциально могут оказать влияние на их достижение. Процесс менеджмента риска предоставляет «разумную» гарантию (если более точно, то определенное основание для уверенности) того, что руководство компании имеет правильно организованный процесс выбора и формирования целей и эти цели соответствуют задачам организации и ее готовность идти на риск.

– Определение событий. Внутренние и внешние события, оказывающие влияние на достижение целей организации, должны определяться с учетом их разделения на риски (потери) или возможности (благоприятное стечение обстоятельств, «улыбнулась удача» и т. п.). Возможности должны учитываться руководством в процессе формирования стратегии и постановки целей.

– Оценка рисков. Риски анализируются с учетом вероятности их возникновения и влияния с целью определения того, какие действия в отношении них необходимо предпринять. Риски оцениваются с точки зрения присущего (характерного) и остаточного риска.

– Реагирование на риск. Руководство выбирает метод реагирования на риск – уход от риска, принятие, снижение или перенос (перераспределение) риска, – разрабатывая ряд мероприятий, которые позволяют привести выявленный риск в соответствие с допустимым уровнем риска и готовностью организации рисковать.

– Средства контроля. Политики и процедуры разработаны и установлены таким образом, чтобы обеспечивать «разумную» гарантию того, что реагирование на возникающий риск происходит эффективно и своевременно.

– Информация и коммуникации. Необходимая информация определяется, фиксируется и передается в такой форме и в такие сроки, которые позволяют сотрудникам выполнять их функциональные обязанности. Также осуществляется эффективный обмен информацией в рамках организации как по вертикали сверху вниз и снизу вверх, так и по горизонтали.

– Мониторинг. Весь процесс управления рисками организации отслеживается и по необходимости корректируется и совершенствуется. Мониторинг осуществляется в рамках текущей деятельности руководства или путем проведения периодических оценок.

Система внутреннего контроля организации позиционируется как составная часть процесса менеджмента риска организации. Менеджмент риска на уровне организации рассматривается как процесс более широкий, чем внутренний контроль. Он включает и развивает систему внутреннего контроля, преобразуя ее в более эффективную форму, акцентированную на риск. В свою очередь менеджмент риска рассматривается как часть общекорпоративного менеджмента.

Современные международные стандарты внутреннего аудита предполагают возможность аудита и оценки как систем внутреннего контроля организации, так и их систем

менеджмента риска. Например, стандарт Института внутренних аудиторов (The Institute of Internal Auditors, IIA) в срезе деятельности IIA 2110 определяет целью проводимых подразделениями внутреннего аудита мероприятий осуществление мониторинга и оценки эффективности действующей в организации системы менеджмента риска. В частности, подразделениям внутреннего аудита вменяется в обязанности оценки степени риска, связанного с действиями руководства организации, ее операционной деятельностью и функционированием ее информационных систем с точки зрения:

– эффективности и результативности операций;

– надежности и достоверности финансовой и оперативной информации;

– сохранности активов;

– соблюдения законов, регламентов и контрактов.

Применительно к информационной сфере организации модель Комитета COSO развивается рядом опять же «стандартов де-факто», таких как COBIT и ITIL. Базовые решения методологии ITIL закреплены отдельными международными стандартами менеджмента услуг информационных технологий в организации из соответствующего семейства стандартов менеджмента ISO/IEC 20000 [21].

Каждая из спецификаций стандартов COBIT и ITIL включает серию объемных документов, подробно останавливаться на которых в формате данного издания не представляется необходимым. Стандарт COBIT претерпел уже 4-ю редакцию (в 2007 г. опубликована редакция 4.1), а спецификация ITIL – 3-ю.

В целом оба из отмеченных стандартизированных подходов (COBIT и ITIL) преследуют следующие общие цели использования информационных технологий в организациях:

– соответствие требованиям, предъявляемым высшим руководством организации;

– обеспечение прозрачности влияния на бизнес и рисков, связанных с ИТ;

– создание механизмов, гарантирующих достижение поставленных целей;

– повышение эффективности реакций на требования бизнеса и изменения в стратегии организации;

– обеспечение эффективной трансляции бизнес-требований в соответствующие возможности решений в сфере информационных технологий;

– интеграция приложений и информационных технологий в бизнес-процессы организации;

– обеспечение эффективных взаимоотношений с другими организациями;

– обеспечение прозрачности ИТ-расходов, потенциала, стратегии, политики и качества услуг;

– обеспечение учета и эффективного использования всех ИТ-активов;

– увеличение эффективности инвестиций в ИТ и вклада информационных технологий в общую эффективность бизнеса;

– оптимизация ИТ-инфраструктуры и ресурсов;

– обеспечение достоверности выполняемых автоматизированных транзакций;

– обеспечение адекватного противодействия ИТ неблагоприятным внешним и внутренним факторам;

– обеспечение требуемой доступности ИТ-услуг;

– поддержка целостности информации и инфраструктуры;

– обеспечение соответствия ИТ-деятельности законам и регулирующим нормам;

– обеспечение стабильного качества услуг, поддержка процесса непрерывного совершенствования.

Все перечисленные позиции органично развивают положения модели Комитета COSO, предлагая риск-ориентированный прагматичный подход к использованию организациями информационных технологий в контексте пользы и выгоды организации от их применения.

Оба стандарта базируются на модели непрерывного совершенствования (в спецификации ITIL явно указано на соответствие модели ИСО 9000; стандарт COBIT подобных формулировок не содержит, но фактически им соответствует).

Во введении стандарта COBIT отмечается, что его структура максимально адаптирована к поддержке структуре контроля для корпоративного управления организации и управления риском, изложенный в рекомендациях Комиссии COSO «Внутренний контроль – Интегрированная структура» и аналогичным руководствам.

Фундаментальным различием COBIT и ITIL является их происхождение, а следовательно, и специфика использования.

Заказчиком и спонсором спецификации ITIL являлись организации, использующие в своей деятельности информационные технологии. С позиций классики модели деятельности организации ИТ реализуют сервисную (вспомогательную) функцию к процессам формирования добавочной стоимости продукции и процессам корпоративного управления. Исключением может быть ситуация, когда основной целью деятельности организации является предоставление ИТ-услуг. Такие компании также присутствуют на рынке, но, как правило, для целей обслуживания крупного «материального бизнеса» (нефтяного или машиностроительного холдинга и т. п.). В таком видении вклада ИТ в обеспечение деятельности организации наиболее уместной представляется сервисная модель организации и реализации процессов менеджмента ИТ в организации со всеми вытекающими сущностями сервисной модели (планирование сервисов, требования к сервисам и т. п.). Именно такая модель положена в основу спецификации ITIL.

Положения стандарта COBIT не отвергают сервисной модели, даже рекомендуют ее к использованию совместно с COBIT. Однако общий взгляд на ИТ в стандарте COBIT несколько иной. Он как бы акцентируется на вопросах интеграции ИТ в общекорпоративный менеджмент, всецелом удовлетворении бизнес-требований и широком охвате контролем достижения целей. В положениях стандарта COBIT отмечается, что структура мер контроля COBIT способствует удовлетворению потребности системы внутреннего контроля организации посредством следующего:

– обеспечения связи с бизнес-требованиями;

– систематизации ИТ-деятельности в виде общепризнанной процессной модели;

– идентификации основных ИТ-ресурсов, которые должны использоваться;

– определения целей контроля управления, которые должны рассматриваться.

Для организации в целом, использование рекомендаций COBIT обеспечивает основу для:

– создания измеримой связи между бизнес-требованиями и ИТ-целями;

– предоставления инструментальных средств для руководства;

– установления целей и метрик, позволяющих оценивать функционирование ИТ;

– использования моделей зрелости, позволяющих проводить сравнительный анализ возможностей процессов;

– применения ролевых нотаций «Ответственность, подотчетность, консультирование и информирование» для прояснения ролей и обязанностей персонала организации.

В качестве преимуществ реализации COBIT как структуры корпоративного управления ИТ в стандарте отмечается:

– лучшая синхронизация бизнеса и ИТ на основе сосредоточения на бизнесе;

– общее понимание среди всех причастных сторон, основанное на общем языке;

– понимание бизнес-руководством того, что поддерживается и реализуется средствами ИТ;

– четкие обязанности и принципы владения на основе процессной ориент ации;

– широкое признание третьими сторонами и регулятивными органами;

– удовлетворение требований COSO для среды контроля ИТ.

Общую спецификацию процессов COBIT иллюстрирует рис. 47.

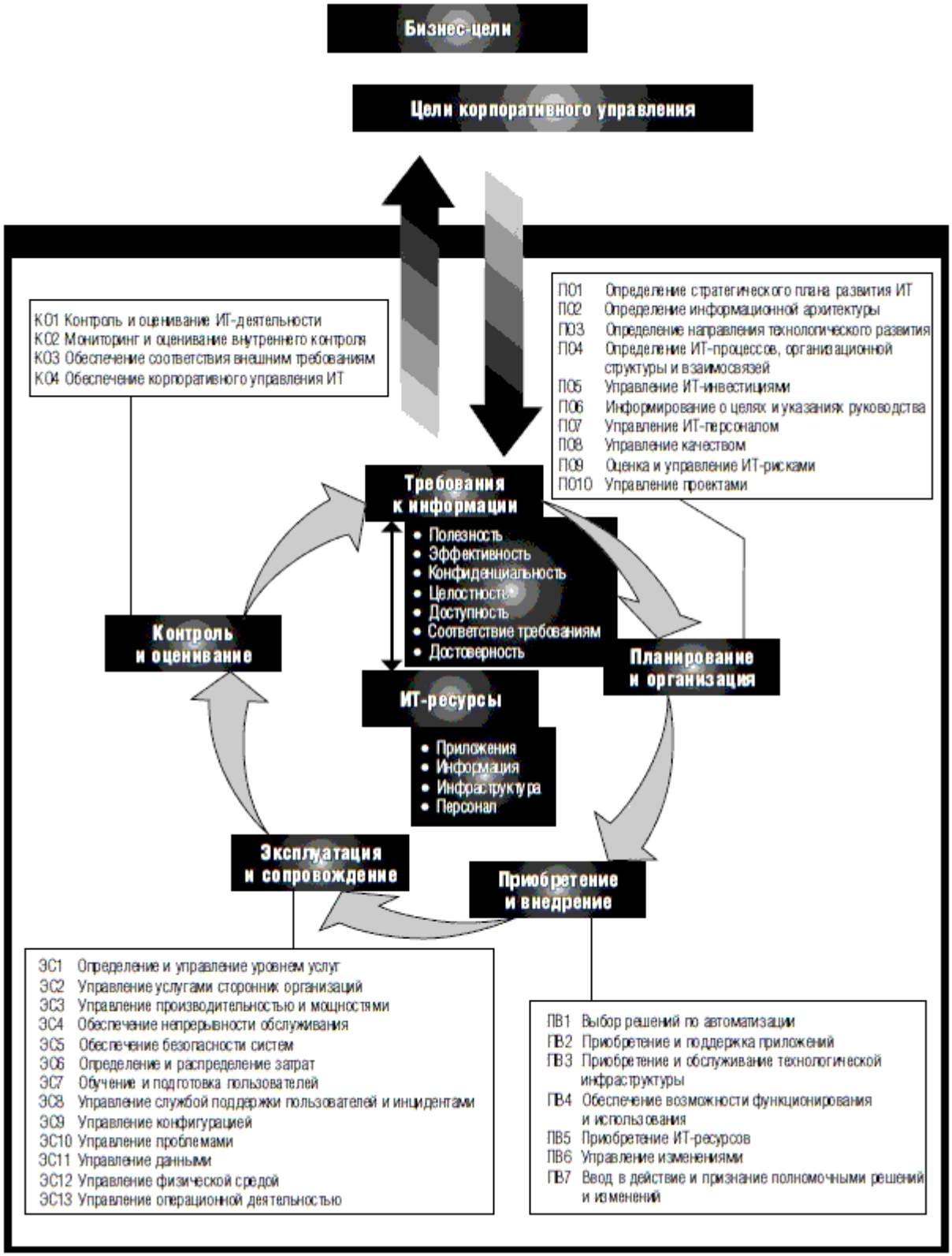


Рис. 47. Спецификация процессов COBIT

Комплекс документов стандарта COBIT включает руководства для многих заинтересованных сторон. Документы COBIT систематизированы по следующим трем уровням (см. рис. 48), предназначенным для поддержки:

– исполнительного высшего руководства организации и правления;

– бизнес-руководителей и ИТ-руководства;

– специалистов в сфере корпоративного управления, доверия, контроля и безопасности.

Рис. 48. Структура документов COBIT

Существуют также производные продукты (руководства) для определенных целей, например, документы, которые рассматривают:

– цели контроля ИТ (на основе COBIT) для Закона Сарбейнса – Оксли;

– базовый уровень безопасности и менеджмент информационной безопасностью COBIT: руководство для совета директоров и исполнительного руководства;

– руководство к COBIT для малых и средних предприятий или больших предприятий, стремящихся достичь более широкой реализации корпоративного управления ИТ.

Все компоненты COBIT взаимосвязаны и предназначены для поддержки потребностей в корпоративном управлении, управлении, контроле и доверии различных заинтересованных сторон (см. рис. 49).

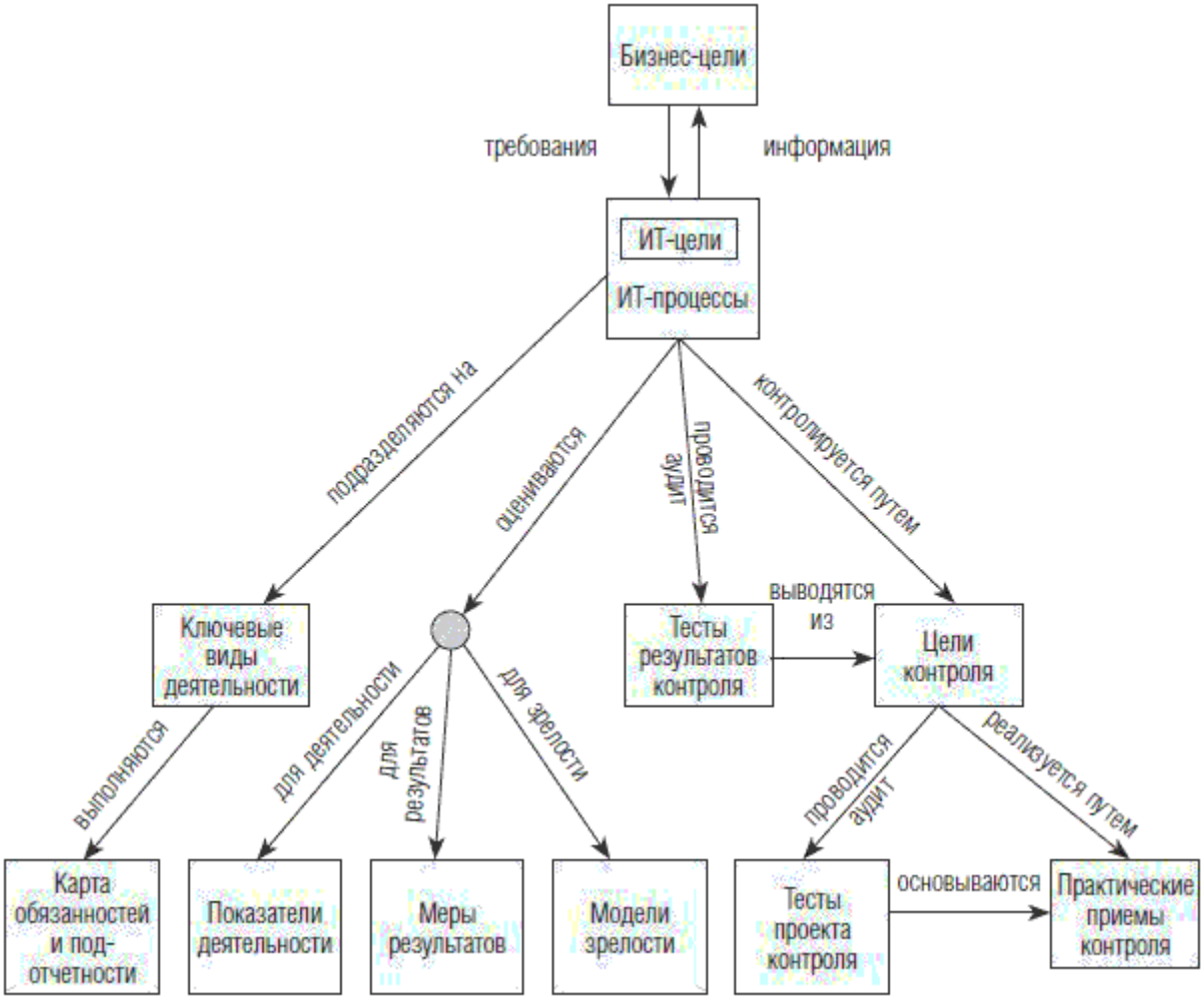


Рис. 49. Взаимосвязи компонентов COBIT

COBIT – это структура и совокупность поддерживающих механизмов и технологий, которые позволяют руководителям ликвидировать расхождения в отношении требований контроля, технических вопросов и бизнес-рисков и информировать об этом уровне контроля причастные стороны.

Практическая сторона использования любой рассмотренной стандартизированной спецификации ИТ, как COBIT, так и ITIL и иных подобных, в конечном случае сопряжена с оценками и измерениями в операционной среде организации. Только информация контроля может показать, насколько планы предприятия реализованы. Только данные по измерениям могут показать «на сколько» планы реализованы или перевыполнены. Тот же COBIT иллюстрирует данный тезис, как показано на рис. 50.

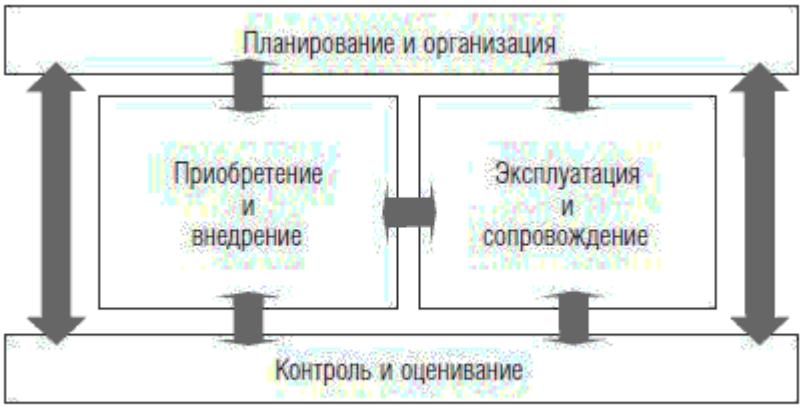


Рис. 50. Роль процессов контроля и оценивания в спецификации стандарта COBIT

В конечном итоге информация контроля и данные измерений и оценки имеют ценность в организации ровно настолько, насколько ее способна «переварить» система корпоративного контроля и управления.

Измеренное (оцененное) значение «0,8», «40», «70 %» без контекста, сопровождающего данное значение оценки, абсолютно бесполезно для системы принятия решений организации (надо что-то делать или, может, подождать). Более того, оно вредно, так как сопровождается затратой ресурсов организации (операционной среды и системы управления), если только наличие какой-либо оценки не является основной целью такой оценки.

В вопросах совершенствования необходимы сведения об ожиданиях (целях и задачах), имевших место при планировании работ. Тогда контроль и измерения в таких условиях сопровождаются платформой и семантикой предполагаемой шкалы и методов контроля и измерения.

При следовании организацией рекомендациям модели Комитета COSO в системе корпоративного менеджмента функциональные и обеспечивающие подразделения, а также ее высшее руководство получают возможность использования в своей практике соответствующих их деятельности моделей непрерывного совершенствования. Наряду с этим и высшее руководство потенциально способно эффективно управлять и адекватно реагировать на события в своей операционной среде и среде бизнеса своей организации. В таких условиях возможно максимально эффективное использование практически любого стандартизированного решения, реализующего модели непрерывного совершенствования, как для сферы обеспечения информационной безопасности бизнеса, так и для информатизации и контроля информационных технологий. Более того, это позволяет выстраивать максимально эффективные и результативные «горизонтальные» связи, например, между подразделениями информатизации и безопасности в контексте общих принципов корпоративного менеджмента и контроля достижения целей деятельности организации.

Далее рассмотрим возможные подходы к измерениям и контролю в моделях непрерывного совершенствования, включая совершенствования системы менеджменты информационной безопасности бизнеса.

2.4. Контроль и аудит (оценки, измерения) в моделях менеджмента (управления)

Измерения и контроль в моделях менеджмента предназначены для удовлетворения информационных потребностей тех или иных заинтересованных сторон в информации, касающейся функционирования объекта измерения и контроля. Все результаты измерений и контроля имеют информационную природу. Потребители информации (заинтересованные стороны) могут быть как внутренними (органы управления и контроля, сервисные

подразделения и т. п.), так и внешними (собственники/акционеры, органы надзора и регулирования, инвесторы и т. д.) по отношению к организации.

В вопросах совершенствования деятельности организации информация измерений и контроля необходима в том числе и для актуализации виртуальной модели материального мира, используемой органами управления в системе принятия решений. В случаях, если поступающие данные от измерений и контроля в организации «не ложатся» (не находят своего места) в виртуальной модели материального мира органа управления, они не могут быть им использованы, а следовательно, являются бесполезными. В связи с этим все затраты организации на осуществление таких измерений можно относить к ущербу (упущенной выгоде, уменьшенной добавочной стоимости и т. п.).

«Классические» рекомендации по роли информации в управлении организацией можно найти во многих известных стандартах, например, таких как ГОСТ Р ИСО 9004. В них отмечается, что лица органов управления должны обращаться с данными как с фундаментальным источником для преобразования в информацию и постоянного развития базы знаний организации, которая важна при принятии решений, основанных на фактах. Это среди прочего может стимулировать нововведения, инновации, объективную основу для решений по совершенствованию деятельности. Для этого органам управления организацией следует:

– определить потребности в информации (категориях и типах, формах ее представления);

– преобразовывать информацию в знания, используемые в организации;

– проводить оценку выгод, получаемых за счет использования информации, с целью улучшения менеджмента информации и знаний организации.

В то же время неэффективно и неадекватно спроектированные измерения и меры контроля могут сформировать ложную уверенность в надлежащем (правильном, эффективном, адекватном условиям и т. д.) функционировании объекта контроля, что способно привести к еще большим издержкам организации.

Какие результаты дает произвольная система измерений, мы можем видеть на улицах российских городов. Метрики контроля эффективности деятельности, устанавливаемые для сотрудников патрульно-постовой службы, инспекторов безопасности дорожного движения, зачастую далеки от факторов, оказывающих действенное влияние на снижение уличной преступности и безопасности на дорогах. Подобные проблемы не являются характерными только для российской действительности. Например, Г. Нив в своей книге [6] приводит пример, когда Деминг показывает ему заголовок из одной газеты: «***Констебль виновен в неисполнении обязанностей – не выполнил план по арестам».*** За это невыполнение полицейский из Торонто был смещен с должности.

Этот достаточно наглядный пример приведен в пятой части книги Г. Нива «Четырнадцать пунктов снова перед нами», где он рассматривает с практической стороны «работу» 14 принципов программы Деминга для менеджмента, иллюстрируя их характерными примерами. Материалы данной главы Нива и других, могут быть полезны всем, кто не на словах, а на деле желает что-либо изменить в лучшую сторону в своей управленческой деятельности.

Что касается рассматриваемого вопроса, то в принципах программы Деминга для менеджмента ожидаемо нашлось место и вопросам измерения и контроля. В главе 29 «Пункт 11: исключите произвольные количественные цели» ярко и на примерах рассмотрены ситуации и последствия поверхностного и непродуманного подхода к измерениям и сформулированы соответствующие рекомендации. Где-то они носят идеалистический характер, но многие из них вполне практичны. Например, нельзя не согласиться с тезисом Деминга «***Измерения – всегда только верхушка айсберга».***

В срезе моделей менеджмента (управления) информационных технологий в организации и систем обеспечения информационной безопасности организаций практически

все стандартизированные для целей проектирования и реализации измерений решения основываются на единой эталонной структуре, отражающей сущности предметной области измерений и их отношения. В каждом конкретном случае все сущности предметной области измерений имеют свое наполнение или решения «по умолчанию».

Рис. 51 иллюстрирует обобщенную модель измерений в системах менеджмента информационных технологий и информационной безопасности организации.

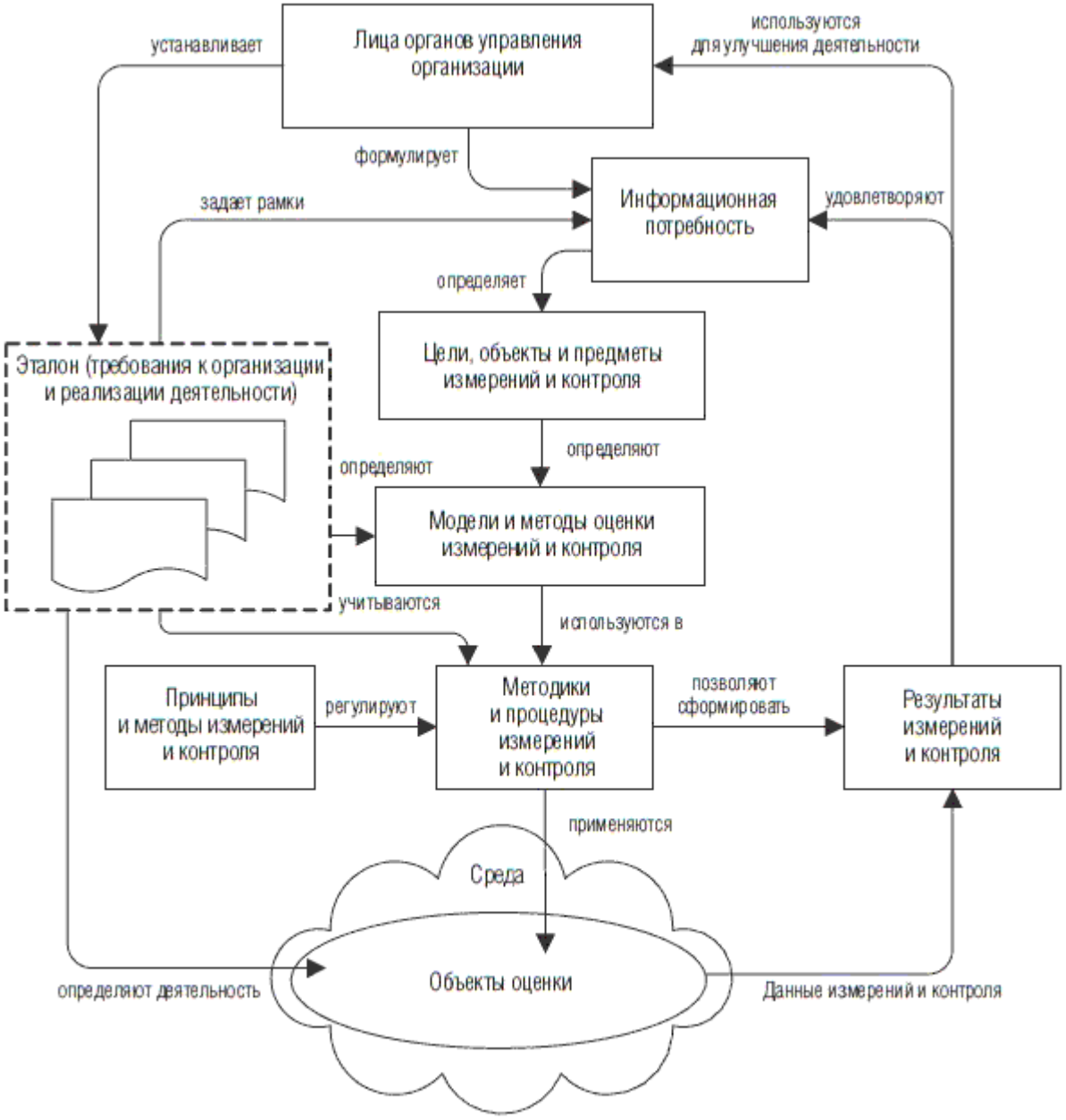


Рис. 51. Обобщенная модель измерений в системах менеджмента ИТ и ИБ организации

Лица органов управления организации соответствующего уровня устанавливают нормы и требования к организации и реализации деятельности в подразделениях организации (эталон), отражающие видение руководства того, что и как должно осуществляться в подразделениях организации для достижения поставленных целей. Это может включать нормы и требования организации функционирования и совершенствования деятельности объекта, нормы и требования риск-менеджмента объекта и т. д. Установление лицами органов управления организации норм и требований к организации и реализации деятельности в подразделениях организации порождает потребность контроля их исполнения и измерений достигнутых результатов.

Задачи контроля и измерений достигнутых результатов формулируются в терминах

информационной потребности в информации результатов тех или иных видов оценок. Потребность представляет собой понимание, включающее необходимость выявления и разрешения целей, задач, рисков и проблем. Для реализации данной потребности определяются цели, объекты и предмет измерений и контроля. Они наряду с эталоном предопределяют модель оценки, включающую установление того, что и как может быть проверено, учитывая аспекты достоверности и правила реализации сбора сведений и их анализа, оценивания (вычисления качественных и /или количественных значений) и интерпретации результатов.

Модели и методы измерений и контроля могут быть отражены в любой форме, в том числе и в виде отдельного документа. Уровень формализации моделей и методов измерений и контроля может быть любым, при условии, что он позволяет использовать данные модели и методы в операционной среде организации на объектах оценки. Композиция эталона и оценочной модели и методов измерений и контроля образуют основу для формирования и использования методической базы (методики, регламенты, инструментальные средства), что формирует основания для проведения практической деятельности на объектах. Эталон в обязательном порядке должен учитываться при формировании методик оценки объекта, так как в противном случае будет затруднительно отобразить и интерпретировать результаты измерений и контроля в терминах того, что должно было быть выполнено на объекте относительно результатов измерений.

Методическое обеспечение определяет структуру и форму результатов измерений и контроля, которые должны удовлетворять потребностям лиц органов управления организации и могут быть интерпретированы для дальнейшего использования. Применение методик на объектах в условиях регламентированных процедур, отвечающих установленным и признаваемым в организации принципам и методам измерений и контроля, должно позволить сформировать результат требуемого качества, удовлетворяющего информационным потребностям.

Результаты измерений и контроля, формируемые на основе полученных с объекта данных измерений и контроля, должны отвечать заявленной информационной потребности и позволять использовать их лицами органов управления организации для совершенствования деятельности (или в иных целях, например, для передачи третьим лицам).

Важным моментом для практики инициирования новых видов проверок (измерений и способов контроля и оценки) является адекватность текущего установленного эталона (действующих норм и требований, предопределяющих деятельность объектов оценки) сформулированной информационной потребности. Существующий эталон, устанавливая правила функционирования объекта, одновременно задает рамки ограничений на возможные информационные потребности лиц органов управления организации в оценочных категориях и возможные ожидания, имеющиеся относительно различных видов измерений и контроля.

Так, например, на практике встречаются ситуации, когда лица органов управления организации в силу различных обстоятельств формулируют потребности в проверках и оценках по некоторой общепризнанной стандартизированной модели (COBIT, ITIL, ISO/IEC 27001, ISO/IEC 20000 и т. д.). В этом случае, если текущая деятельность организации (существующий эталон) определяет порядок разработки, поставки и внедрения систем организации по требованиям стандартов иных стандартов, например комплексов стандартов ГОСТ 34, ГОСТ 2, ГОСТ 19, то результат может быть далек от ожиданий (соответствия). Результаты оценки не выведут на соответствие, а зачастую не покажут вообще ничего (значение оценки будет «ноль»). Это, как правило, лишний раз доказывает лишь то, что модели и методы измерений должны органично развивать требования эталона и быть с ним совместимым.

Ряд стандартизированных решений менеджмента ИТ и ИБ организации наряду с требованиями менеджмента включает и критерии и методы измерений и контроля (оценки). Среди них можно отметь те же COBIT и ITIL, ISO/IEC 27001, международные стандарты процессного подхода (процессов жизненного цикла ИТ) 15288 (систем) и 12207

(программного обеспечения) и др.

Для целей измерений в стандартах процессного подхода (процессов жизненного цикла ИТ) 15288 (систем) и 12207 (программного обеспечения) еще в 2002 г. был принят международный стандарт ISO/IEC 15939 [22] «Проектирование систем и программного обеспечения – процесс измерения» (пересмотренный пять лет спустя). Данный международный стандарт определяет мероприятия и задачи, необходимые для реализации процесса измерения. Мероприятие – это совокупность взаимосвязанных задач, способствующая достижению назначения и результатов процесса измерения. Задача – строго определенная часть работы. Каждое мероприятие состоит из одной или более задач. Модель процесса измерений по ISO/IEC 15939 иллюстрирует рис. 52.

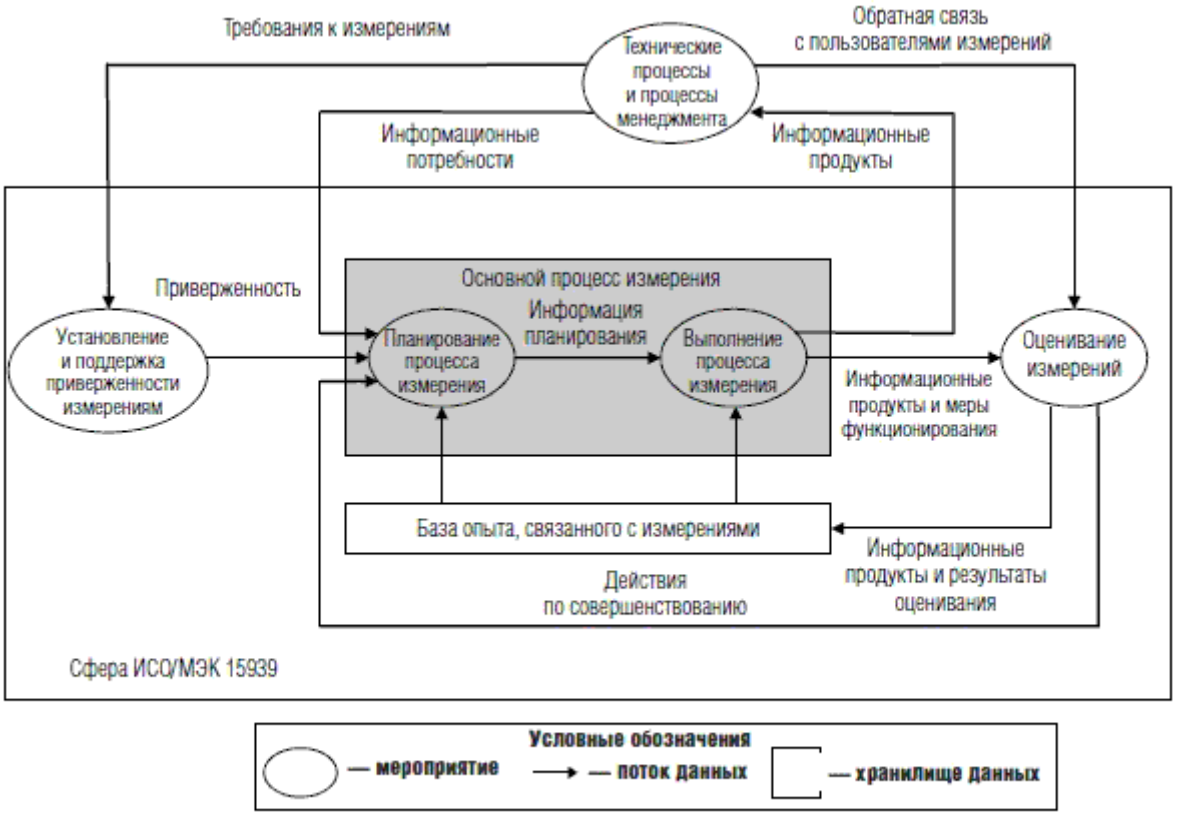


Рис. 52. Модель процесса измерения

Как показано на рис. 52, процесс измерений по ISO/IEC 15939 включает четыре целевых вида деятельности (мероприятия). Мероприятия упорядочены в итеративном цикле (подобном циклу Деминга), предусматривающем постоянную обратную связь и совершенствование процесса измерения. Работы в рамках мероприятий также являются итеративными.

Блок «Технические процессы и процессы менеджмента» организационной единицы или проекта выходят за рамки положений данного стандарта, хотя они являются важным внешним связующим звеном с мероприятиями измерений. Два мероприятия считаются относящимися к основному процессу измерения: планирование процесса измерения и выполнение процесса измерения. Эти мероприятия в основном уделяют внимание интересам пользователя измерений. Два других мероприятия – установление и поддержка приверженности измерениям и оценивание измерений – обеспечивают основу для основного процесса измерения и обратную связь для него.

В цикл включена «база опыта, связанного с измерениями». Она предназначена для хранения информационных продуктов из прошлых итераций цикла, предыдущих оценок информационных продуктов и оценок предыдущих итераций процесса измерения. Она может включать сведения, которые были сочтены полезными для будущего. Никаких положений о характере или технологии «базы опыта, связанного с измерениями» в стандарте

не дается, предполагается только то, что это постоянное хранилище. Хранящиеся в «базе опыта, связанного с измерениями» сведения предназначены в основном для повторного использования в будущих итерациях процесса измерения.

Типичные функциональные роли, упомянутые в стандарте, включают причастную сторону, организатора, пользователя измерений, аналитика измерений, библиотекаря измерений, поставщика данных и владельца процесса измерения.

В целом же вопросы измерений в СМИБ не столь просты, как может показаться на первый взгляд. Область информационной безопасности, подобно области риск-менеджмента, является чрезвычайно трудной сферой для задач измерений.

Основная проблема заключается в том, ***как измерить «отсутствие инцидентов».***

Вопрос состоит в следующем.

Если анализ рисков информационной безопасности является точным и если мы реализовали эффективные средства контроля и управления ИБ, мы должны избежать или по крайней мере уменьшить число серьезных инцидентов безопасности.

Если мы будем последовательно измерять и фиксировать число и серьезность инцидентов, у нас будут некоторые цифры для анализа, но о чем эти цифры будут фактически говорить нам?

Если эти цифры ниже, чем до начала действия официально утвержденной программы по обеспечению информационной безопасности, мы можем заявить об успехе, но что если число и серьезность инцидентов каким-либо образом снизилось ввиду иных причин, не связанных с нашими усилиями («затаился» агент угроз и т. п.)?

Если цифры выше, чем раньше, обязательно ли это означает, что наши средства контроля и управления неэффективны? Или это может означать, что угрозы и воздействия возросли, а мы их не учли (не видели, неверно оценили актуальность и т. д.)?

Настоящая проблема – это проблема прогноза. Практически невозможно абсолютно достоверно и объективно измерить то, что может произойти в будущем, если бы мы не совершенствовали наши средства контроля и управления информационной безопасности (ничего не меняли бы в своей операционной среде в части средств и мер ИБ).

Измерения ИБ следует вывести из действия общекорпоративной модели системы планирования и отчетности, так как это специфичная задача и она не полностью отвечает методологии прогнозных плановых показателей, применимых к производственной сфере. Вопросы измерений в СМИБ сопоставимы с иными подобными измерениями по форматам категорий отдельных результатов, но решения по ним должны рассматриваться отдельно.

Таким образом, основными вопросами измерения и контроля в СМИБ организации и корпоративном управлении ИБ являются следующие.

Что мы собираемся измерять?

Это, несомненно, важный вопрос, но на практике идентификация надлежащей метрики является по-настоящему сложной. Нам необходимо учитывать следующие практические правила:

– не следует реализовывать процесс измерений, если мы не намерены регулярно и систематически его поддерживать, необходимы воспроизводимые и надежные методы измерений;

– не следует собирать данные, которые мы не намерены анализировать, – это нерациональные расходы, которых можно избежать;

– не следует анализировать данные, если мы не намерены практически использовать результаты анализа, другими словами, нам необходимо идентифицировать информационные потребности в результатах измерений.

Мы можем достичь многого без дорогостоящих решений или сложных измерительных процессов. Не следует углубляться в частные вопросы. Вопросы материально-технического обеспечение сбора данных для измерений могут быть организованы на основе уже имеющейся в других подразделениях организации сведений (см. пример по измерению

осведомленности ИБ). Следует лишь удостовериться в том, что они формируются на основе регламентированных процедур и их достоверность может быть проверена и подтверждена.

Как мы будем осуществлять измерения?

Это подразумевает следующие вопросы: откуда мы получаем данные для измерений и контроля и где они будут храниться? Если исходная информация еще не доступна для измерений, то необходимо реализовать процессы для ее сбора. Это, в свою очередь, связано с вопросом о том, кто будет собирать данные (новая работа должна быть обоснована потенциальной выгодой организации от ее выполнения). Предполагает ли это централизованные или распределенные процессы сбора данных? Если источниками данных будут отделы и подразделения, находящиеся вне вашего контроля, то насколько достоверными могут быть эти сведения (возможны ли манипуляции цифрами)? Будут ли они отвечать вашим требованиям по форматам и срокам предоставления? Насколько вы можете автоматизировать сбор и обработку данных, встроив, например, отчет о безопасности в отчеты прикладных системы?

Как мы будем осуществлять отчетность?

Чего действительно ожидает высшее руководство? Необходимо обсудить назначение и ожидаемые результаты измерений с руководителями и сотрудниками смежных подразделений. Следует придерживаться принципа «от простого к сложному». Система неизбежно будет развиваться. Следует начать с простых (типовых для практики организации), понятных отчетов, развивая их далее с учетом рекомендаций руководства. Если система отчетности измерений проектируется «с нуля», то есть возможность вариаций, может существовать возможность предоставления отчетности отличным от других направлений отчетности в организации образом, используя иные форматы представления и оформления содержания.

Как мы должны реализовывать систему измерений и отчетности?

Разрабатывая метрики (структура, шкала, модели и методы измерений), следует оценить осуществимость и эффективность процессов измерений и полезность выбранной метрики в ограниченном масштабе, прежде чем развертывать их во всей организации. То, что хорошо выглядит в теории, может не оказаться эффективным в практике. Экспериментальные исследования и опытная эксплуатация являются уместным методом отработки оптимальных конфигураций в процессах сбора и анализа, принятия решения о том, является ли метрика действительно наглядной для принятия решений по итогам измерений.

Являются ли данные достаточно точными? Может не требоваться совершенная точность, но определенно необходимым является то, чтобы цифры были правдоподобными и воспроизводимыми. Следует ожидать, что руководству могут быть необходимы сведения об источнике данных, процедурах их сбора, анализа и формах представления.

Далее рассмотрим, как работают процессы аудита в функциях контроля обеспечения информационной безопасности бизнеса.

3. Оценка информационной безопасности бизнеса. Проблема измерения и оценивания информационной безопасности бизнеса

3.1. Способы оценки информационной безопасности

Организации, бизнес которых во многом зависит от информационной сферы, для достижения целей бизнеса должны поддерживать на необходимом уровне систему обеспечения ИБ (СОИБ). СОИБ представляет собой совокупность аппаратно-программных, технических и организационных защитных мер (ЗМ), функционирующих под управлением СМИБ и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту ИБ.

Желание иметь СОИБ, адекватную целям ИБ организации по обеспечению доступности, целостности и конфиденциальности информационных активов, приводит к стремлению совершенствовать СОИБ. Совершенствование, улучшение СОИБ возможно при условии знания состояний характеристик и параметров используемых ЗМ, процессов менеджмента, осознания ИБ и понимания степени их соответствия требуемым результатам. Понять эти аспекты СОИБ можно только по результатам оценки ИБ организации, полученной с помощью модели оценки ИБ на основании свидетельств оценки, критериев оценки и с учетом контекста оценки.

Критерии оценки – это все то, что позволяет установить значения оценки для объекта оценки. В качестве критериев оценки ИБ могут использоваться требования ИБ, процедуры ИБ, сочетание требований и процедур ИБ, уровень инвестиций, затрат на ИБ.

К свидетельствам оценки ИБ относятся записи, изложение фактов или любая информация, которая имеет отношение к критериям оценки ИБ и может быть проверена. Такими свидетельствами оценки ИБ могут быть доказательства выполняемой и выполненной деятельности по обеспечению ИБ в виде отчетных, нормативных, распорядительных документов, результатов опросов, наблюдений.

Контекст оценки ИБ объединяет цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли.

Модель оценки ИБ определяет сферу оценки, отражающую контекст оценки ИБ в рамках критерия оценки ИБ, отображение и преобразование оценки в параметры объекта оценки, а также устанавливает показатели, обеспечивающие оценку ИБ в сфере оценки.

В общем виде процесс проведения оценки ИБ (рис. 53) представлен основными компонентами процесса: контекст, свидетельства, критерии и модель оценки, – необходимыми для реализации процесса оценки.

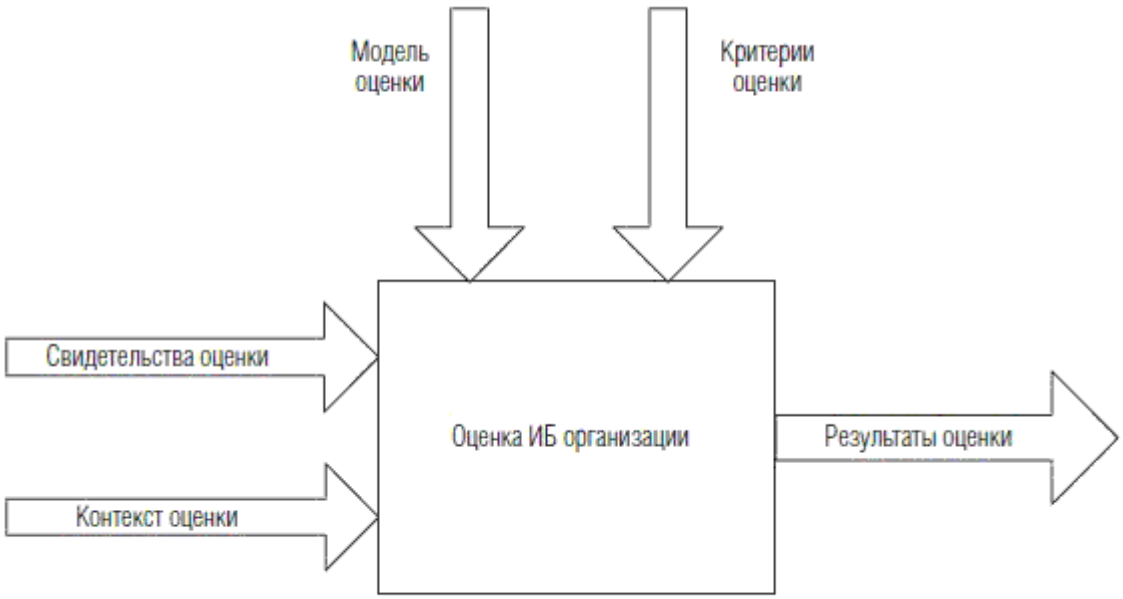


Рис. 53. Общий вид процесса оценки ИБ организации

Оценка ИБ заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения ИБ, адекватности используемых защитных мер или целесообразности (достаточности) инвестиций (затрат) для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических элементов (факторов) объекта оценки.

Наряду с важнейшим назначением оценки ИБ – создание информационной потребности для совершенствования ИБ, возможны и другие цели проведения оценки ИБ такие, как:

– определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов обеспечения ИБ, защитных мер;

– выявление влияния критических элементов (факторов) и их сочетания на ИБ организации;

– сравнение зрелости различных процессов обеспечения ИБ и сравнение степени соответствия различных защитных мер установленным требованиям.

Результаты оценки ИБ организации могут также использоваться заинтересованной стороной для сравнения уровня ИБ организаций с одинаковым бизнесом и сопоставимым масштабом.

В зависимости от выбранного для оценки ИБ критерия можно разделить способы оценки ИБ организации (рис. 54) на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

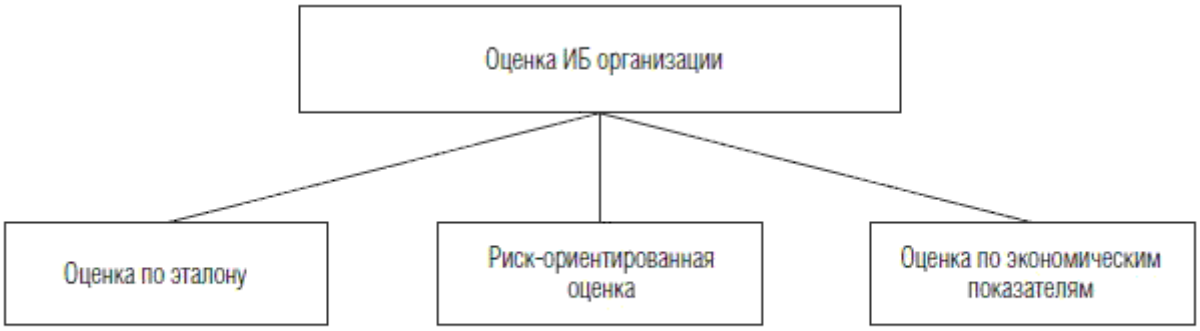


Рис. 54. Способы оценки ИБ организации

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела проводится оценка соответствия СОИБ организации установленному эталону. Под оценкой соответствия ИБ организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ организации и идентифицируются недостатки такой реализации.

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия СОИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

– требования законодательства Российской Федерации в области ИБ;

– отраслевые требования по обеспечению ИБ;

– требования нормативных, методических и организационно-распорядительных документов по обеспечению ИБ;

– требования национальных и международных стандартов в области ИБ.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки ИБ, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки ИБ.

Риск-ориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков ИБ, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков ИБ, формирование на их основе критериев оценки ИБ, сбор свидетельств оценки и измерение риск-факторов, формирование оценки ИБ.

Способ оценки ИБ на основе экономических показателей оперирует понятными для

бизнеса аргументами о необходимости обеспечения и совершенствования ИБ. Для проведения оценки в качестве критериев эффективности СОИБ используются, например, показатели совокупной стоимости владения (Total Cost of Ownership – TCO) [24].

Под показателем TCO понимается сумма прямых и косвенных затрат на внедрение, эксплуатацию и сопровождение СОИБ. Под прямыми затратами понимаются все материальные затраты, такие как покупка оборудования и программного обеспечения, трудозатраты соответствующих категорий сотрудников. Косвенными являются все затраты на обслуживание СОИБ, а также потери от произошедших инцидентов. Сбор и анализ статистики по структуре прямых и косвенных затрат проводится, как правило, в течение года. Полученные данные оцениваются по ряду критериев с показателями TCO аналогичных организаций отрасли.

Оценка на основе показателя TCO позволяет оценить затраты на информационную безопасность и сравнить ИБ организации с типовым профилем защиты, а также управлять затратами для достижения требуемого уровня защищенности.

Основные этапы оценки эффективности СОИБ на основе модели TCO включают сбор данных о текущем уровне TCO, анализ областей обеспечения ИБ, выбор сравнимой модели TCO в качестве критерия оценки, сравнение показателей с критерием оценки, формирование оценки ИБ.

Однако этот способ оценки требует создания общей информационной базы данных об эффективности СОИБ организаций схожего бизнеса и постоянной поддержки базы данных в актуальном состоянии. Такое информационное взаимодействие организаций, как правило, не соответствует целям бизнеса. Поэтому оценка ИБ на основе показателя TCO практически не применяется.

Далее рассмотрим подробнее способ оценки ИБ на основе эталона и способ риск-ориентированной оценки ИБ.

3.2. Процесс оценки информационной безопасности

3.2.1. Основные элементы процесса оценки

Процесс оценки ИБ включает следующие элементы проведения оценки:

– контекст оценки, который определяет входные данные: цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки, а также роли и ресурсы;

– критерии оценки;

– модель оценки;

– мероприятия процесса оценки: сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов объекта оценки;

– выходные данные оценки.

Основные элементы процесса оценки ИБ [25] представлены на рис. 55 в виде процессной модели.

Прежде чем рассмотреть особенности способов оценки ИБ организации необходимо описать общие для любой оценки ИБ компоненты: контекст оценки, сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов при проведении оценки различного вида (независимая оценка, самооценка) и выходные данные оценки. Модель оценки и критерии оценки, определяющие особенности способов оценки, будут рассмотрены в других разделах.

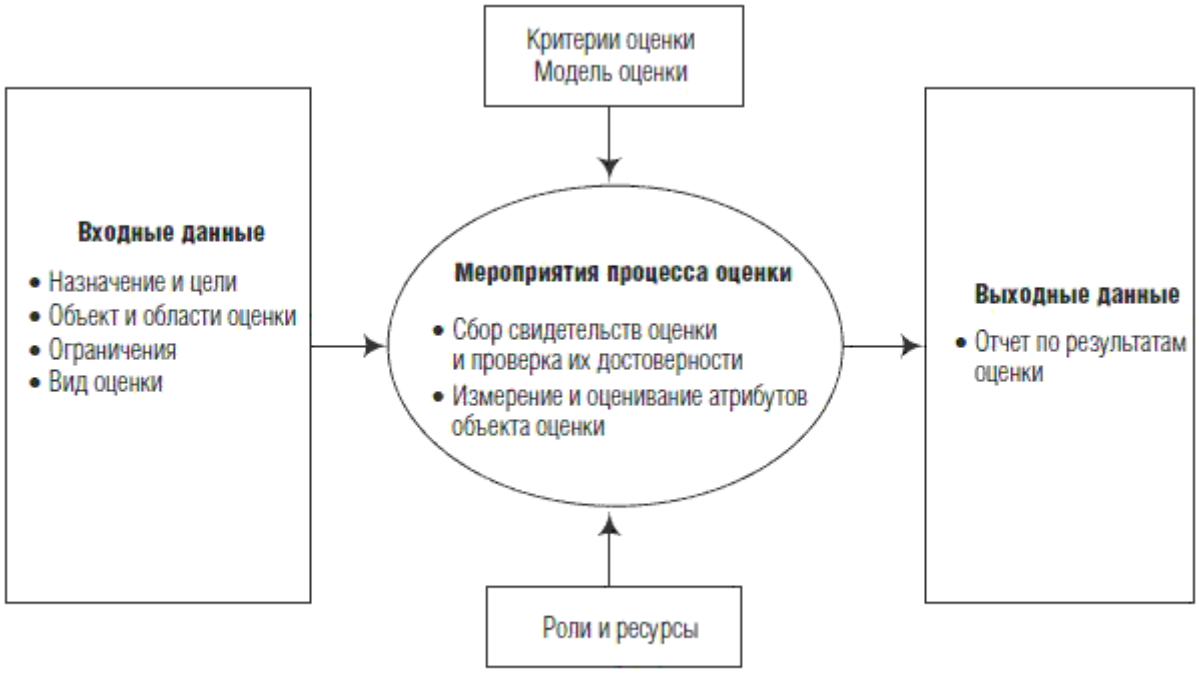


Рис. 55. Основные элементы процесса оценки ИБ

Рассмотрим подробнее элементы процесса оценки ИБ организации.

3.2.2. Контекст оценки информационной безопасности организации

Контекст оценки ИБ включает цели и назначение оценки ИБ, вид оценки, объект и области оценки ИБ, ограничения оценки, роли и ресурсы.

К ролям, участвующим в реализации процесса оценки, относятся организатор, аналитик, руководитель группы оценки, оценщик, владелец активов, представитель объекта оценки.

Организатор (заказчик) оценки ИБ формирует цель оценки (совершенствование объекта оценки, определение соответствия объекта оценки установленным критериям и т. д.) и определяет критерий оценки, объект и область оценки. Под организатором оценки понимается лицо или организация, являющиеся внутренними или внешними по отношению к оцениваемому объекту оценки, которые организуют проведения оценки и предоставляют финансовые и другие ресурсы, необходимые для ее проведения. Организатор должен обеспечить доступ группы оценки (руководитель группы оценки, оценщик) к активам объекта оценки для изучения, к персоналу для проведения опросов, к инфраструктуре, необходимой во время оценивания. Хотя руководство объекта оценки напрямую не имеет никаких конкретных обязанностей по проведению оценивания, осознание важности оценки имеет очень большое значение. Это особенно актуально в том случае, когда организатор оценки не является членом руководства объекта оценки.

По завершении оценки организатор передает отчетные документы по оценке заинтересованным сторонам для использования их в соответствии с заявленной целью оценки.

Аналитик оценки ИБ выбирает способ оценки ИБ, модель оценки и определяет методическое и информационное обеспечение оценки, т. е. методики, данные для оценки. Аналитик оценки анализирует результаты оценки и формирует отчет и рекомендации по результатам оценки ИБ.

Руководитель группы оценки и оценщик измеряют и оценивают свидетельства оценки, предоставленные владельцами активов, и формируют результаты оценки. Руководитель группы должен распределить ответственность между членами группы за оценивание конкретных процессов, подразделений, областей или видов деятельности объекта оценки.

Такое распределение должно учитывать потребность в независимости, компетентности специалистов по оценке и результативном использовании ресурсов. Мероприятия по измерению и оцениванию выполняются исключительно руководителем группы оценки и оценщиком, входящими в группу оценки. Другой персонал (представитель объекта оценки, технический эксперт) может участвовать в работе группы оценки для обеспечения специализированных знаний или консультаций. Они могут обсуждать с оценщиком формулировки суждений, но не будут нести ответственность за окончательную оценку.

На рис. 56 показаны роли процесса оценки ИБ и основные функции, выполняемые ролями.

Важным аспектом при определении контекста оценки является вид оценки: независимая или самооценка. В зависимости от вида оценки различается отношение ролей процесса оценки и объекта оценки.

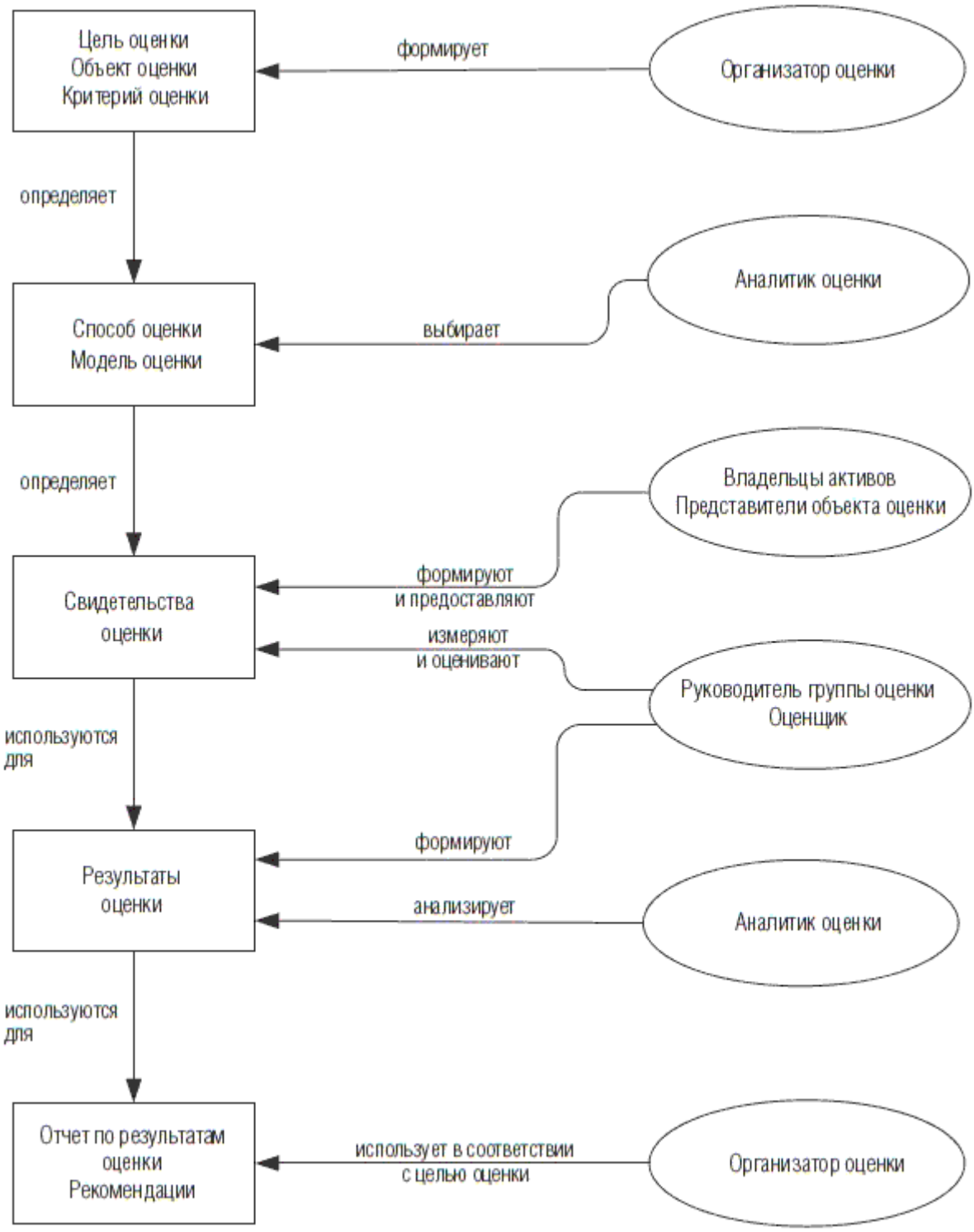


Рис. 56. Роли процесса оценки ИБ и их функции

Независимая оценка достигается путем проведения оценки группой оценки, члены которой независимы от объекта оценки. Организатор оценки может относиться к той же организации, к которой относится объект оценки, но не обязательно к оцениваемому объекту оценки. Степень независимости может варьироваться в соответствии с целью и областью оценки. В случае внешнего организатора оценки предполагается наличие взаимного соглашения между организатором оценки и организацией, к которой относится объект оценки. Представитель объекта оценки принимает участие в формировании свидетельств оценки, обеспечивает взаимодействие группы оценки с владельцами активов. Их участие в проведении оценки дает возможность определить и учесть особенности объекта оценки,

обеспечить достоверность результатов. Самооценка выполняется организацией с целью оценки собственной СОИБ. Организатор самооценки обычно входит в состав объекта оценки, как и члены группы оценки.

Область оценки может включать, например, один или несколько процессов объекта оценки, например, организатор может сосредоточить внимание на одном или нескольких критических процессах и /или защитных мерах. Выбор объекта оценки должен отражать намеченное использование организатором выходных данных оценки. Например, если выходные данные предназначены для использования при совершенствовании деятельности по обеспечению ИБ, то область оценки должна соответствовать области намеченных работ по совершенствованию. Область оценки может быть любой: от отдельного процесса до всей организации. В контексте оценки должно быть представлено подробное описание объекта оценки, включающее размеры объекта оценки, область применения продуктов или услуг объекта оценки, основные характеристики (например, объем, критичность, сложность и качество) продуктов или услуг объекта оценки.

К ограничениям оценки можно отнести возможную недоступность основных активов, используемых в обычной деловой деятельности организации; недостаточный временной интервал, выделенный для проведения оценивания; необходимость исключения определенных частей объекта оценки из-за стадии жизненного цикла. Кроме того, могут быть наложены ограничения на количество и вид данных, которые должны быть собраны и изучены.

Содержание контекста оценки должно быть согласовано руководителем группы оценки с организатором и уполномоченным представителем объекта оценки и задокументировано до начала процесса оценки. Фиксирование контекста оценки важно, так как он содержит исходные элементы процесса оценки.

Во время выполнения оценки могут происходить изменения в контексте оценки. Изменения должны быть одобрены организатором оценки и уполномоченным представителем объекта оценки. Если эти изменения оказывают влияние на временной график и ресурсы проведения оценки, то планирование оценки должно быть соответствующим образом пересмотрено.

3.2.3. Мероприятия и выходные данные процесса оценки

Сбор свидетельств оценки и проверка их достоверности. Назначение мероприятия: сбор свидетельств оценки с соблюдением условий обеспечения достоверной оценки ИБ.

Независимая оценка ИБ может быть осуществлена с помощью внутреннего и внешнего аудита ИБ. В [26] аудит ИБ определяется как систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ, установления степени выполнения в организации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения об информационной безопасности организации.

Необходимыми условиями обеспечения достоверной оценки ИБ при проведении аудита являются:

– использование доверенного процесса аудита и соблюдение основных принципов аудита;

– менеджмент программы аудита ИБ;

– использование наиболее достоверных источников свидетельств оценки;

– определение объема выборки с учетом заданной достоверности свидетельств оценки;

– учет факторов, влияющих на аудиторский риск, с целью снижения аудиторского риска.

Доверенный процесс аудита ИБ должен отвечать требованиям принятого в организации нормативного документа, описывающего процесс аудита ИБ, либо требованиям

признаваемого сообществом международного (национального) нормативного документа (стандарта, рекомендации). Таким нормативным документом для банковской системы РФ является СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности», принятый и введенный в действие распоряжением Банка России от 28 апреля 2007 г. № Р-345. В стандарте изложены принципы проведения аудита ИБ организации, описана последовательность этапов проведения аудита ИБ, установлены требования к этапам проведения аудита ИБ организаций и к взаимоотношениям представителей аудиторской организации с представителями проверяемой организации.

В СТО БР ИББС-1.1-2007 изложено также содержание программы аудита ИБ, включающей деятельность, необходимую для планирования и организации определенного количества и вида аудитов и обеспечения их ресурсами, необходимыми для эффективного и результативного проведения аудитов в заданные сроки. В стандарте определены процедуры менеджмента программы аудита ИБ, направленные на контроль внедрения программы аудита ИБ, анализ достижения целей программы аудита ИБ и определение возможностей для ее совершенствования. Совершенствование программы аудита ИБ состоит в определении корректирующих и превентивных действий по совершенствованию программы аудита ИБ, включающих в себя пересмотр и корректировку сроков проведения аудитов ИБ и необходимых ресурсов, улучшение методов подготовки свидетельств аудита ИБ.

К основным принципам проведения аудита ИБ [27] относятся:

– независимость аудита ИБ: аудиторы (группа оценки) независимы в своей деятельности и не ответственны за деятельность, которая подвергается аудиту ИБ, независимость является основанием для беспристрастности при проведении аудита ИБ и объективности при формировании заключения по результатам аудита ИБ;

– полнота аудита ИБ: аудит ИБ должен охватывать все области аудита ИБ, соответствующие цели оценки, кроме того, полнота аудита ИБ определяется достаточностью затребованных и предоставленных материалов, документов и уровнем их соответствия поставленным задачам; полнота аудита ИБ является необходимым условием для формирования объективных заключений по результатам оценки ИБ;

– оценка на основе свидетельств аудита ИБ: при периодическом проведении аудита ИБ оценка на основе свидетельств аудита ИБ является единственным способом, позволяющим получить повторяемое заключение по результатам аудита ИБ, что повышает доверие к такому заключению, для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми;

– достоверность свидетельств аудита ИБ: оценщики должны быть уверены в достоверности свидетельств оценки ИБ, доверие к документальным свидетельствам оценки ИБ повышается при подтверждении их достоверности третьей стороной или руководством организации; доверие к фактам, полученным при опросе сотрудников объекта оценки, повышается при подтверждении данных фактов из различных источников, доверие к фактам, полученным при наблюдении за деятельностью в области ИБ объекта оценки, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов;

– компетентность и этичность поведения: доверие к процессу и результатам оценки ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения; компетентность базируется на способности аудитора применять знания и навыки; этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, беспристрастность.

Соблюдение принципов проведения аудита ИБ является предпосылкой для объективных заключений по результатам оценки.

Основными методами получения свидетельств оценки должны быть:

– проверка и анализ документов, относящихся к объекту оценки;

– наблюдение за процессами объекта оценки;
– опрос сотрудников объекта оценки и независимой (третьей) стороны.

Наряду с ручными способами сбора информации формирование свидетельств аудита может быть автоматическим или полуавтоматическим в результате применения какого-то инструментального средства или применения нескольких инструментальных средств.

При сборе данных оценщики должны исходить из того, что деятельность по обеспечению ИБ в области оценки осуществляется в соответствии с критериями оценки ИБ, если этому есть доказательства. Оценщики должны проявлять достаточную степень профессионального скептицизма в отношении собираемых свидетельств оценки, принимая во внимание возможность наличия нарушений ИБ.

Проверка и анализ документов позволяют оценщику получить свидетельства оценки, обладающие наибольшей полнотой и удобством восприятия и использования по сравнению с другими методами получения свидетельств аудита. Однако эти свидетельства аудита имеют различную степень достоверности в зависимости от их характера и источника, а также от эффективности контроля за процессом подготовки и обработки представленных документов.

Свидетельствами оценки ИБ, полученными в результате проверки и анализа документов, могут быть:

– наличие документа (документов) с релевантным содержанием;
– выдержки из документа (документов), подтверждающие реализацию деятельности по обеспечению ИБ, возложение ответственности и обязанностей на сотрудника (сотрудников) за реализацию деятельности по обеспечению ИБ;
– выдержки из документа (документов), содержащие описания реализованных ЗМ, процессов обеспечения ИБ.

Наблюдение представляет собой отслеживание оценщиком процедур или процессов обеспечения ИБ, выполняемых другими лицами (в том числе персоналом организации). Информация считается достоверной только в том случае, если получена непосредственно в момент функционирования проверяемых процедур или процессов.

Свидетельствами аудита, полученными с помощью наблюдения за деятельностью, могут быть записи, факты или другая информация, имеющие отношение к результатам автоматического контроля техническими средствами, зафиксированные оценщиками в ходе наблюдения.

Устный опрос проводят оценщики среди сотрудников (владельцев активов), утвержденных представителем объекта оценки для предоставления источников свидетельств и свидетельств оценки. Результаты устных опросов должны оформляться в виде протокола или краткого конспекта, в котором обязательно должны быть указаны фамилия, имя, отчество оценщика, проводившего опрос, фамилия, имя, отчество опрашиваемого лица, а также их подписи. Для проведения типовых опросов могут быть подготовлены бланки с перечнями интересующих вопросов. Результаты устного опроса следует проверять, так как опрашиваемый может выражать свое субъективное мнение.

Свидетельствами аудита, полученными при проведении опроса, могут быть описания и разъяснения опрашиваемых лиц по реализации процессов, процедур по обеспечению ИБ.

Для уверенности в достоверности оценки оценщики должны быть уверены в достоверности выявленных свидетельств аудита. Собранные свидетельства оценки, используемые для оценивания показателей, должны быть точным представлением оцениваемого объекта оценки. Для этого следует учитывать достоверность источников свидетельств аудита.

По степени достоверности (от наибольшей к наименьшей) источники свидетельств оценки делятся на:

– документальные источники свидетельств, полученные из различных источников третьей стороны (сведения об использовании лицензионных мер и средств обеспечения ИБ,

договора по сопровождению мер и средств обеспечения ИБ и т. д.);

– документальные источники свидетельств, полученные на (от) объекте (та) оценки и подтвержденные третьей стороной (план мероприятий по результатам внешнего аудита ИБ, материалы ведомственных проверок ИБ и т. д.);

– источники свидетельств, полученные в ходе проведения аудиторских процедур, не предусматривающих периодическую документальную отчетность (результаты наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т. д.);

– источники свидетельств, полученные в виде нормативных и распорядительных документов (политики, регламенты, отчеты о деятельности, приказы, распоряжения и т. д.), указывающих на надлежащее применение процессов и мер обеспечения ИБ на практике (наличие разрешительных записей уполномоченных лиц, данных контроля рисков и т. д.);

– свидетельства, полученные в результате устных и письменных опросов об объекте оценки, и наблюдение за применением мер и средств обеспечения ИБ, которые не оставляют документальных свидетельств (выявление ролей процессов, последовательности применения ЗМ и т. д.).

Наряду с достоверностью источников свидетельств следует учитывать временной период получения свидетельств и сочетание источников свидетельств оценки. Например, доверие к фактам, полученным при наблюдении за деятельностью, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов; доверие к фактам, полученным при опросе сотрудников, повышается при подтверждении данных фактов из различных источников.

Достоверность выявленных свидетельств оценки ИБ зависит также от объема выборки при формировании свидетельств оценки. Соответствующее использование объема выборки тесно связано с доверием, с которым относятся к заключениям по результатам аудита.

Некоторые свидетельства оценки основано на выборках релевантных данных. Например, свидетельства наличия ЗМ для всех систем, степени охвата персонала и сотрудников подразделения процессами обучения и осведомления ИБ и т. д. Выборка производится с целью измерения и оценивания менее чем 100 % объектов проверяемой совокупности. Задачей оценщика при проведении выборки является определение наиболее оптимального способа отбора элементов для формирования свидетельств оценки. При этом возможно:

– отобрать все элементы (сплошная проверка);

– отобрать специфические (определенные) элементы;

– отобрать отдельные элементы (сформировать аудиторскую выборку).

Сплошная проверка целесообразна, если:

– генеральная совокупность состоит из небольшого числа элементов большой стоимости;

– риск контроля является высоким, а другие средства не позволяют получить достаточные свидетельства оценки;

– повторяющийся характер расчетов или иных процессов делает сплошную проверку эффективной с точки зрения соотношения затрат и результатов.

Сплошная проверка редко применяется при проведении оценки ИБ.

Оценщик может решить отобрать специфические (определенные) элементы генеральной совокупности, основываясь на том, что они могут включать:

– элементы с высокой стоимостью или так называемые критические (ключевые) элементы выборки;

– элементы, стоимость которых превышает определенную величину;

– элементы для проверки процедур, позволяющие определить, выполняется ли организацией конкретная процедура.

Выводы по результатам измерения, применяемого к отобранным таким способом элементам, не могут быть распространены на всю генеральную совокупность. При использовании этого метода анализируется потребность в получении свидетельств оценки в отношении оставшейся части генеральной совокупности, если оставшаяся часть является существенной.

Оценщик с учетом имеющихся сведений может принять решение о проведении выборочной проверки путем отбора отдельных элементов, т. е. применить статистический подход. Общее требование в этом случае – репрезентативность, т. е. все элементы изучаемой генеральной совокупности должны иметь равную вероятность быть отобранными в выборку.

При применении методов, связанных со статистической выборкой, объем отобранной совокупности может определяться на основании теории вероятностей и математической статистики либо профессионального суждения аудитора.

Достоверность оценки во многом зависит от того, как будут оценщиками учтены факторы, влияющие на аудиторский риск, который включает:

– риск контроля;

– риск необнаружения.

Риск контроля представляет собой риск того, что внутренний контроль не предотвратит или не выявит существенных нарушений ИБ. Важным фактором для повышения достоверности оценок является оптимизация объема выборки в соответствии с предполагаемым риском контроля.

Риск необнаружения представляет собой риск того, что процедуры и методы аудита, применяемые оценщиками, не выявят существенных нарушений.

Важными факторами для снижения риска необнаружения и тем самым повышения достоверности оценок являются:

– увеличение времени проверки;

– проведение опросов, ориентированных на представителей третьих независимых лиц;

– увеличение объема выборки.

Измерение и оценивание атрибутов объекта оценки. Назначение мероприятия: измерение и оценивание атрибутов объекта оценки на основе свидетельств оценки ИБ с целью установления степени выполнения критериев оценки и формирования отчета по результатам оценки.

Атрибут представляет собой свойство или характеристику сущности, которые могут быть определены количественно или качественно ручными или автоматическими средствами.

Для рассмотрения процесса измерения и оценивания атрибутов объекта оценки ИБ воспользуемся моделью измерений, связанных с обеспечением ИБ, представленной на рис. 57.

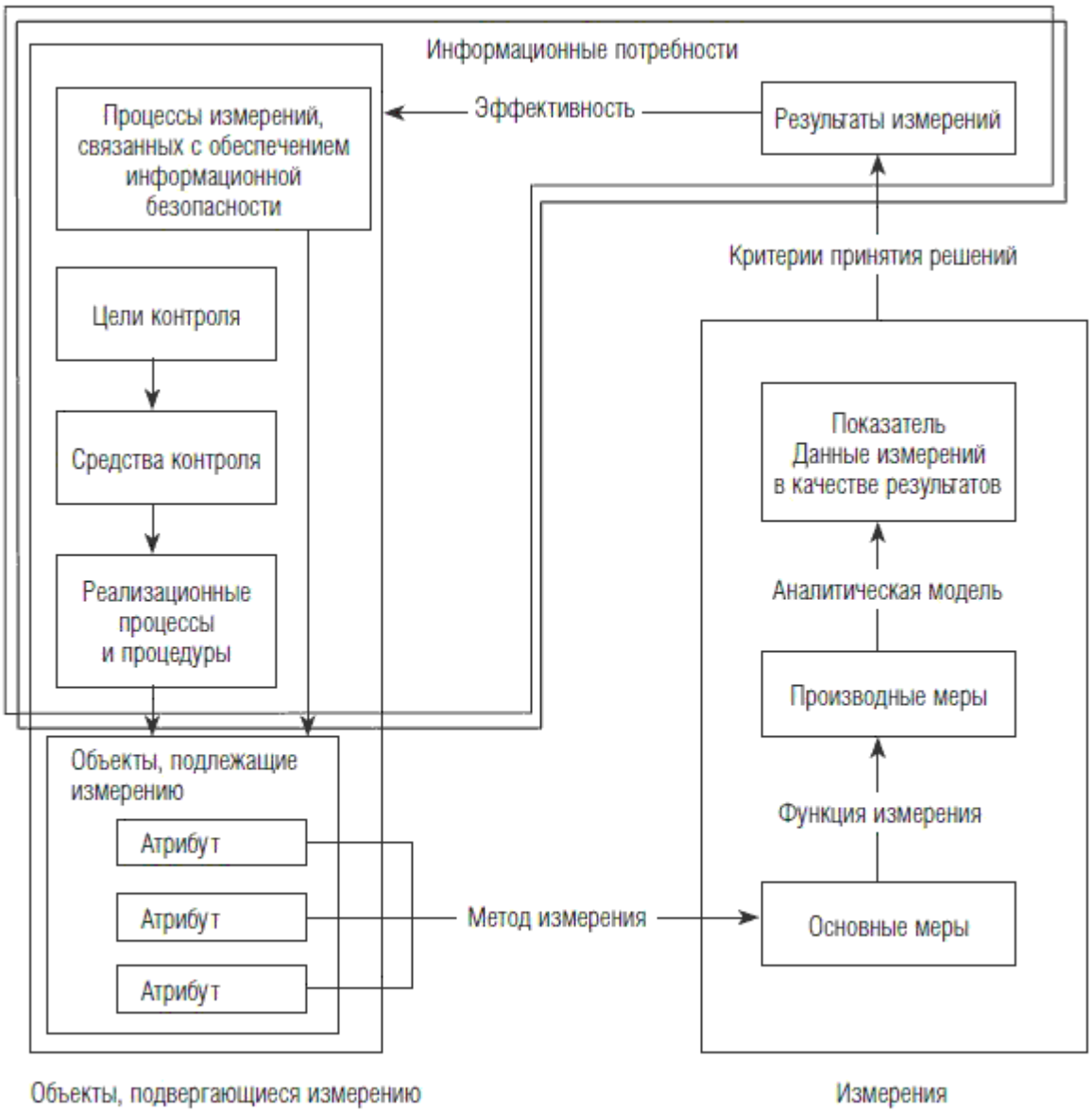


Рис. 57. Модель измерений, связанных с обеспечением ИБ

Информационная потребность определяет, что требуется измерить для достижения целей оценки ИБ объекта оценки. Измерения, связанные с обеспечением ИБ, могут применяться к различным объектам в рамках контекста оценки. Для идентификации объектов измерения выделяются критические атрибуты процессов, процедур, защитных мер, которые могут предоставить данные, соответствующие информационной потребности.

Метод измерения используется для количественного измерения объекта измерения посредством преобразования атрибутов в основную меру. Основная мера – мера, определенная в терминах атрибута и метода его количественного определения (мера – это переменная, которой присваивается значение). Основная мера функционально независима от других мер. Основная мера собирает информацию о единственном атрибуте.

Метод измерения количественно измеряет атрибуты посредством применения соответствующей шкалы.

Методы измерения могут быть субъективными или объективными. Субъективные методы полагаются на количественное измерение, включающее мнение человека, тогда как объективные методы используют количественное определение, основанное на числовых правилах, которые могут быть реализованы с помощью ручных или автоматических средств.

Функция измерения определяет, как основные меры объединяются в производную меру. Производная мера – способ объединения двух или более основных мер.

Функции измерения могут включать разнообразные приемы, такие как усреднение всех основных мер, применение весовых коэффициентов к основным мерам или присвоение качественных значений основным мерам перед их объединением в производные меры.

Для каждой меры должна быть определена аналитическая модель с целью преобразования одной или более производных мер в показатель. Показатель – это результат применения аналитической модели к одной или более мерам по отношению к критериям принятия решений или информационной потребности.

Показатели будут формироваться путем объединения производных мер и интерпретации их на основе критериев принятия решений.

Для каждого показателя должны быть идентифицированы и задокументированы основанные на целях информационной безопасности критерии принятия решений, которые устанавливают максимальное значение показателя, и предоставляют руководство для интерпретации текущего значения показателя.

В таблицах 3–6 показаны примеры проведения измерения и оценивания атрибута.

Таблица 3

Объект измерения	Атрибут	Метод измерения	Основная мера
База данных служащих	Записи, относящиеся к служащим	1) Запрос базы данных для извлечения числа служащих из базы данных отслеживания обучения и повышения осознания. 2) Запрос базы данных для извлечения числа служащих, подписавших соглашения с пользователями. 3) Запрос базы данных для извлечения числа служащих, подписавших соглашения с пользователями, из базы данных отслеживания обучения и повышения осознания. 4) Запрос базы данных для извлечения общего числа служащих	1) Число служащих, получивших обучение, направленное на повышение осознания безопасности. 2) Число служащих, подписавших соглашения с пользователями. 3) Число служащих, получивших обучение, направленное на повышение осознания безопасности, и подписавших соглашения с пользователями. 4) Общее число служащих

Таблица 4

Основные меры	Функция измерения	Производная мера
1) Число служащих, получивших обучение, направленное на повышение осознания безопасности, и подписавших соглашения с пользователями. 2) Число служащих, подписавших соглашения с пользователями	1) Разделить число служащих, получивших обучение, направленное на повышение осознания безопасности, и подписавших соглашения с пользователями, на число служащих, подписавших соглашения с пользователями, и умножить на 100% 2) Разделить число служащих, подписавших соглашения с пользователями, на общее число служащих и умножить на 100%	1) Процентное отношение служащих, получивших обучение, направленное на повышение осознания безопасности, и подписавших соглашения с пользователями. 2) Процентное отношение служащих, подписавших соглашения с пользователями

Таблица 5

Производные меры	Аналитическая модель	Показатель
1) Процентное отношение служащих, получивших обучение, направленное на повышение осознания безопасности, и подписавших соглашения с пользователями.	X = определенное пороговое значение для соответствия политике, приемлемое для организации.	Красный, желтый, зеленый или линейный график, представляющий тенденцию результатов измерений в течение многих отчетных периодов.

Окончание табл. 5

Производные меры	Аналитическая модель	Показатель
2) Процентное отношение служащих, подписавших соглашения с пользователями	Предполагается, что значение показателя является красным. Если X% служащих подписало соглашение с пользователями, значение показателя становится желтым. Если X% служащих получило обучение, направленное на повышение осознания безопасности, и подписало соглашения с пользователями, значение показателя становится зеленым	Когда линия пересекает пороговые значения, цвет на графике меняется в соответствии с аналитической моделью

Таблица 6

Показатели	Критерии принятия решений	Результат измерений
Красный, желтый, зеленый или линейный график, представляющий тенденцию результатов измерений в течение многих отчетных периодов. Когда линия пересекает пороговые значения, цвет на графике меняется в соответствии с аналитической моделью	Зеленый — соответствие политике. Желтый или красный — несоответствие политике. Возрастающая тенденция указывает на улучшение соответствия, убывающая тенденция — на ухудшение соответствия. Наклон может дать понимание эффективности реализации средств контроля. Резкие изменения наклона в любом направлении указывают, что реализация средств контроля требует внимательного изучения для определения причины. Негативные тенденции могут требовать вмешательства руководства. Позитивные тенденции должны быть изучены для идентификации потенциальных лучших практических приемов	Соответствующее требованиям и эффективное средство контроля не требует изменений. Соответствующее требованиям, но неэффективное средство контроля должно быть рассмотрено на предмет исправления. Несоответствующее требованиям и неэффективное средство контроля требует усовершенствования

Сообщение результатов оценки может проходить неформально при внутренней оценке или происходить в форме подробного отчета при независимой внешней оценке. Кроме того, для представления результатов оценки могут быть подготовлены и другие выводы и предлагаемые планы действий, рекомендации, в зависимости от назначения оценки. Результаты могут быть представлены в абсолютных выражениях или в относительных выражениях в сравнении с результатами предыдущих оценок, контрольными данными, в сравнении с деловыми потребностями и т. д. Результаты оценки ИБ обычно используются в качестве основы для определения рисков ИБ и разработки плана совершенствования СОИБ.

Выходные данные оценки включают дату проведения оценки, входные данные оценки, собранные свидетельства оценки, описание используемого процесса измерения и оценивания. Зарегистрированные выходные данные оценки могут сохраняться в различной форме – бумажной или электронной – в зависимости от обстоятельств и инструментов, использованных для проведения и поддержки оценки.

На основе любого соглашения об обеспечении конфиденциальности или ограничений доступа зарегистрированные данные могут сохраняться организатором оценки или руководством объекта оценки.

Важные факторы достижения цели оценки ИБ следующие:

– осознание и мотивация руководства организации;

– конфиденциальность;

– доверие.

Позиция руководства организации оказывает существенное влияние на процесс оценки. Поэтому руководство организации должно побуждать участников оценки к открытости и конструктивности. Оценка объекта сосредотачивается на оценке процессов, процедур, защитных мер, а не на функционировании персонала объекта оценки. Смысл оценки состоит в том, чтобы сделать объект оценки более эффективными в достижении целей бизнеса, а не в том, чтобы возложить вину на отдельных лиц.

Обеспечение обратной связи и поддержка атмосферы, поощряющей открытое обсуждение предварительных выводов во время оценивания, содействуют обеспечению того, чтобы выходные данные оценки были значимыми для объекта оценки. Руководителям организации и персоналу объекта оценки необходимо осознавать, что участники оценки являются основным источником знаний и опыта, связанных с процессом, и что руководители и персонал имеют хорошую возможность для идентификации потенциальных слабых мест.

Уважение к конфиденциальности источников информации и документации, собранной во время оценивания, необходимо для обеспечения безопасности этой информации. В тех случаях, когда используются опросы или обсуждения, следует обратить внимание на обеспечение того, чтобы их участники не ощущали угрозы или не испытывали какого-либо беспокойства в отношении конфиденциальности. Некоторая из предоставленной информации может составлять собственность организации, поэтому важно наличие адекватных средств контроля для обращения с такой информацией.

Организатор оценки, руководство и персонал объекта оценки должны верить в то, что оценка принесет результат, являющийся объективным для объекта оценки. Важно, чтобы все стороны могли быть уверены в том, что специалисты по оценке обладают адекватными знаниями и опытом для проведения оценки, беспристрастны и обладают адекватным пониманием объекта оценки и его бизнеса для проведения оценки.

3.2.4. Способы измерения атрибутов объекта оценки

Атрибуты, выделенные для измерения как критические элементы процесса, процедуры, защитной меры или объекта оценки, должны быть представлены в удобном для анализа виде с целью адекватного преобразования атрибута в основную меру. Оценщик получает больше возможностей для адекватного представления атрибута основной мерой, если измеряемый атрибут будет дополнен элементами, отражающими контекст оценки.

В настоящее время используются две формы описания измеряемого атрибута: анкеты и метрики.

Для подготовки процесса измерения атрибутов с помощью анкет требуется (см. рис. 58):

– выделить среди атрибутов критические, т. е. те атрибуты, которые позволят достичь цели оценки, и сформировать вопросы анкеты;

– определить с помощью модели оценки способ измерения.

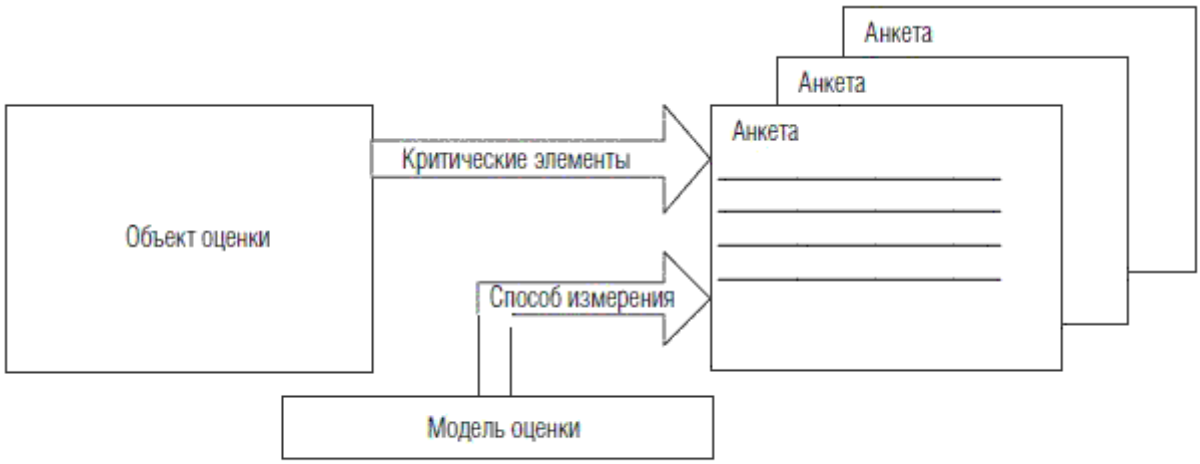


Рис. 58. Формирование анкет для измерения атрибутов

Это позволит оценщику преобразовать измеряемые атрибуты в основные меры при наличии необходимых для измерения источников свидетельств и свидетельств оценки. Отражение контекста оценки в анкете минимально: описание атрибута в виде вопроса. Элементы контекста оценки могут присутствовать в дополнительных методических и

распорядительных документах, обеспечивающих процесс оценки ИБ. В этих документах, как правило, указываются источники свидетельств оценки, а также персонал, ответственный за заполнение анкет. Анкеты могут быть созданы не только для получения основной меры атрибута, но и для формирования производной меры. В этом случае в анкете должна быть определена модель объединения основных мер в производную меру.

Примеры анкет, предназначенных для измерения атрибутов, связанных с информационной безопасностью, рассмотрены, например, в NIST Special Publication 800-26 «Security Self-Assessment Guide for Information Technology Systems» и в BSI PAS 56 [28]. Фрагмент анкеты BSI PAS 56, содержащей атрибуты в виде вопросов, шкалу для измерения атрибутов и модель для объединения основных мер в производную меру, представлен в таблице 7.

Другой подход к измерению атрибутов опирается на применение метрик при измерении атрибутов. Для подготовки процесса измерения атрибутов с помощью метрик требуется (см. рис. 59):

– выделить среди атрибутов критические, т. е. те атрибуты, которые позволят достичь цели оценки;

– определить с помощью модели оценки способ измерения;

– сформировать перечень источников свидетельств оценки и свидетельств оценки, необходимых для измерения атрибутов;

– установить роли и их функции при проведении измерения;

– определить условия функционирования процесса, процедуры, защитной меры или объекта оценки, включающие период сбора, анализа данных, отчетности.

Таблица 7

Фрагмент анкеты BSI PAS 56

Жизненный цикл	Количество вопросов	Номер вопроса	Вопросы	Total NO of returns	Ответы							Среднее значение	Вес вопроса	Общее значение	Соответствие	Комментарии
					«НЕТ» 0%	20%	40%	60%	80%	100%	N/A					
Управление менеджментом непрерывности бизнеса																
	12	*1.1*	*Имеет ли организация четко определенный, документированный, подтвержденный процесс управления программой менеджмента непрерывности бизнеса?*	0									0,08			
		1.2	*Использует ли организация BSI PAS 56 как основу программы менеджмента непрерывности бизнеса?*	0									0,08			
		1.3	*Достигает ли процесс управления программой менеджмента непрерывности бизнеса результата, который приведен в части 5.2.3 BSI PAS 56?*	0									0,08			

При разработке метрик и реализации метрик ИБ должны выполняться следующие условия:

– метрики должны давать результат в количественно измеримой форме (в процентах, в усредненных и абсолютных значениях), например: «процент систем, для которых имеется план работы в чрезвычайной ситуации», «процент уникальных идентификаторов пользователей», «процент систем, в которых применяются запрещенные к использованию протоколы», «процент систем, для которых существуют документированные отчеты об оценке рисков» и т. п.;

– данные для поддержки метрик должны быть доступными;

– значения метрик должны быть достижимы и иметь смысл для бизнеса;

– не следует измерять атрибуты, которые не требуется совершенствовать.

Рис. 59. Формирование метрик для измерения атрибутов

Пример формирования метрик в соответствии со стандартом NIST 800-55 «NIST Special Publication 800-55 «Security Metrics Guide for Information Technology Systems» показан в таблице 8.

Таблица 8

Форма метрик в соответствии со стандартом NIST 800-55

Цель эффективности	Формулируются желаемые результаты, которые должна обеспечить реализация одной или нескольких целей безопасности или методов и средств управления безопасностью системы, которые измеряются метрикой. При использовании NIST SP 800–26 в данный элемент описания метрики следует внести критический (контролируемый) элемент, заданный в NIST SP 800–26

Окончание табл. 8

Задача эффективности	Формулируются действия, которые следует выполнить для достижения цели эффективности. При использовании NIST SP 800–26 в данном элементе должен быть представлен один или несколько дополнительных вопросов, определенных для критичного (контролируемого) элемента в NIST SP 800–26. Для одной цели эффективности может существовать несколько задач эффективности
Метрика	Задается количественная мера, обеспечиваемая метрикой. Используется численное выражение, которое начинается словами «процентное отношение», «число», «частота», «среднее значение» или другие аналогичные термины
Назначение	Описывается общая функциональность, для осуществления которой проводится сбор метрик. Описывается, будет ли метрика использоваться для измерения качества работы внутри организации или для отчетности во внешние контролирующие органы. Также здесь описывается, понимание каких вопросов планируется получить, используя метрики, причины сбора конкретных метрик (регулятивные и законодательные требования), если таковые существуют, и другие аналогичные аспекты
Свидетельство реализации	Перечисляются доказательства существования средств управления безопасностью, которые подтверждают правильность их реализации. Свидетельство реализации используется для вычисления метрики. Свидетельство выступает в качестве косвенного показателя, который подтверждает выполнение деятельности, и в качестве причинных факторов, которые могут указывать на причины неудовлетворительных результатов для конкретной метрики
Частота	Задаются периоды времени для сбора данных, который осуществляется для измерения происходящих изменений. Периоды времени задаются на основе вероятных ожидаемых обновлений, которые могут возникнуть при реализации средств управления
Формула	Описывается способ расчета численного значения метрики. В качестве входных данных для формулы используется информация из перечисленных свидетельств реализации
Источник данных	Перечисляется местонахождение данных, используемых для расчета метрики. Указываются базы данных, средства слежения, подразделения или конкретные роли в организации, которые могут предоставить необходимую информацию
Индикаторы	Предоставляется информация о смысле метрики и ее тренде. Перечисляются возможные причины измеренных трендов и указываются возможные решения для исправления выявленных недостатков. Описывается цель качества работы (эффективности), если она установлена для метрики, и указывается, какие тренды будут считаться положительными в контексте достижения заданной цели. Описывается способ использования информации из свидетельств реализации в качестве входных данных для анализа показателей. Свидетельство реализации служит для подтверждения эффективности деятельностей по обеспечению безопасности и для точного определения причинных факторов

Форма метрик, показанная в таблице 9, подробно описывает объект измерения и атрибут, основную и производную меры, роли и функции ролей при измерении, метод измерения, процедуры сбора и анализа данных.

Таблица 9

Форма метрик в соответствии с ISO/IEC 27004

Идентификация меры	
Название меры	Название меры
Числовой идентификатор	Уникальный, характерный для организации числовой идентификатор
Назначение меры	Описывает причины введения меры
Проверяющий	Лицо или организационная единица, проверяющие, чтобы критерии оценивания мер были соответствующими для верификации эффективности средств контроля
Объекты измерения и атрибуты	
Объект измерения	Объект, подлежащий измерению. Объекты могут включать процессы, системы или компоненты систем
Атрибуты	Свойство или характеристика объекта измерения, которые могут быть определены количественно или качественно ручными или автоматическими средствами
Спецификация основной меры (для каждой основной меры)	
Основные меры	Основная мера — это мера единственного атрибута, определенная посредством специфицированного метода измерения (например, число обученных членов персонала, количество площадок, совокупные расходы на данный момент). Когда данные собраны, основной мере присваивается значение
Метод измерения	Логическая последовательность операций, определяющих правило вычисления, для вычисления каждой основной меры. Для основных мер — метод измерения, посредством которого будут получены данные для измерения, включая точность, шкалу и единицы измерения
Шкала	Упорядоченная совокупность значений или категорий, которые используются в основной мере

Спецификация производной меры	
Производная мера	Мера, которая выведена как функция двух или более основных мер
Методы измерения	Формула, которая используется для вычисления производной меры. Для производных мер — функция измерения, посредством которой объединяются производные меры, на основе соответствующих основных мер и результирующая совокупная точность
Шкала	Упорядоченная совокупность значений или категорий, которые используются в основной мере

Продолжение табл. 9

Спецификация показателя	
Описание и пример показателя	Представление одной или более мер (основных и производных) для поддержки пользователя в получении информации для анализа и принятия решений. Показатель часто представляется как график или диаграмма. Включает общее описание показателя
Аналитическая модель	Процесс, применяющий критерии принятия решений для определения поведенческих реакций на количественные результаты показателей.
Критерии принятия решений	Определенная совокупность действий, которые будут предприняты в ответ на достигнутые количественные значения модели
Интерпретация показателя	Описание того, как интерпретировался примерный показатель (смотри примерное значение в описании показателя)
Эффекты/влияние	Описание эффектов и влияния, выведенных как следствие результатов, полученных путем измерения
Причины отклонения	Определение возможных причин отклонения полученных результатов
Позитивные значения	Формулировка, объясняющая, указывают ли увеличивающиеся значения на позитивные значения (хороший результат) или для указания позитивных значений должны быть взяты уменьшающиеся значения
Форматы отчетности	Должны быть идентифицированы и задокументированы форматы отчетности. Описывает наблюдения, которые организация или владелец информации могут хотеть зафиксировать. Форматы отчетности будут наглядно изображать меры и предоставлять словесное объяснение показателей. Форматы отчетности должны удовлетворять требованиям заказчика информации
Процедура сбора данных	
Частота сбора данных	Как часто осуществляется сбор данных
Владелец информации	Лицо или организация, которые владеют информацией об объектах измерения и атрибутах, используемых для создания основных мер, и которые отвечают за измерения
Сборщик информации	Лицо или организационная единица, отвечающие за сбор, фиксирование и хранение данных
Инструментальные средства, используемые для сбора данных	Перечислите любые инструментальные средства, используемые для сбора данных (например, сканер уязвимостей)
Репозитарий собранных данных	Перечислите любые инструментальные средства, где хранятся данные после их сбора (например, база данных)
Дата сбора	Дата получения данных

Окончание табл. 9

Процедура фиксирования данных	Определяет процедуру фиксирования данных (ссылка на процедуру)
Мера действительна до…	Дата пересмотра (истечение срока или обновление действенности меры)
Период анализа	Определяет измеряемый период
Процедура анализа данных (для каждого показателя)	
Частота сообщения данных	Как часто представляется отчетность по данным (это может происходить реже, чем сбор данных)
Лицо, сообщающее информацию	Лицо или организационная единица, отвечающие за анализ данных и сообщение результатов
Источник данных для анализа	Перечислите любые источники данных для этого анализа
Инструментальные средства, используемые в анализе	Перечислите любые инструментальные средства, используемые для анализа (например, средства статистического анализа)
Заказчик информации	Лицо или организационная единица, запрашивающие и требующие меры в поддержку своих деловых функций

3.3. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности

3.3.1. Модель оценки информационной безопасности на основе оценки процессов

При описании процесса оценки ИБ организации в разделе 3.2 не рассматривалось содержание модели оценки ИБ и критериев оценки ИБ. Эти компоненты процесса оценки ИБ связаны с целью оценки таким образом, что через цель оценки определяется критерий оценки ИБ, в рамках которых (цель, критерий) выбирается модель оценки ИБ организации.

Предположим, что целью оценки ИБ является оценка процессов обеспечения всей организации или объекта (ов) организации. Для достижения такой цели оценки в качестве критерия оценки ИБ должна использоваться эталонная модель процессов обеспечения ИБ, которая описывает в зависимости от объекта оценки совокупность из одного или более процессов в терминах назначения и ожидаемых результатов. Эталонная модель процессов может содержать более подробное описание процессов с выделением атрибутов по назначению и / или ключевых атрибутов – критических элементов процессов.

Модель оценки процесса включает сферу модели, показатели, отображение и преобразование модели оценки процесса.

Сфера модели оценки процесса может распространяться на подмножество процессов, определенных эталонной моделью процессов объекта оценки, а также охватывать дополнительные процессы, выходящие за рамки процессов объекта оценки. Сфера модели оценки может полностью соответствовать эталонной модели процессов объекта оценки.

Модель оценки процесса основывается на совокупности показателей, которые используются в качестве основы для сбора объективных данных для определения степени достижения атрибутов процессов, назначения и результатов процессов в рамках сферы модели оценки процесса. Показатели формализуют процесс оценки, дают возможность

последовательно формировать суждения специалиста по оценке и повышать воспроизводимость результатов. Показатели позволяют оценить степень реализации процессов объекта оценки. Модели оценки процесса в целом обеспечивают различные степени анализа процесса на основе числа показателей оценки, предоставляемых моделью оценки процесса. Модель оценки процесса с 20 показателями оценки будет считаться обеспечивающей более глубокий анализ процесса, чем модель оценки процесса с 10 показателями оценки. Однако такой анализ требует более значительных усилий во время оценки по выявлению данных, касающихся показателей оценки, а затем обработки данных.

Модель оценки процесса должна позволять отображать атрибуты процессов объекта оценки на выбранной шкале. Такой шкалой может быть количественная шкала (например, абсолютная или шкала отношений), которая указывает степень реализации процесса или достижение заданного уровня атрибута процесса, или качественная шкала (например, порядковая), которая указывает на уровень качества процесса.

Показатели, отображая назначения, результаты и атрибуты процессов, формируют таким образом эталонные профили процессов.

Отображение модели оценки процесса должно обеспечивать формальный и поддающийся проверке механизм представления результатов оценки как совокупности параметров процесса для каждого процесса, выбранного из установленной модели (моделей) процесса.

Модель оценки процесса должна обеспечивать четкое преобразование из основных элементов модели в процессы выбранной модели процессов и в соответствующие параметры процесса в структуре измерений.

Преобразование должно быть полным, четким и однозначным. Преобразование показателей в модели оценки процесса должно производиться в:

– назначения и результаты процессов в установленной модели процесса;

– параметры процесса (включая все результаты достижения, перечисленные для каждого параметра процесса) в структуре измерений.

Международный стандарт ИСО/МЭК 15504 [29] определяет, что для оценки процесса могут использоваться модель, оценивающая функционирование процесса, и модель, оценивающая возможности процесса. Измерение функционирования процесса обеспечивается эталонной моделью процесса. Измерение возможности процесса состоит из структуры измерений, включающей шесть уровней возможностей процесса и соответствующие атрибуты процесса.

Разберем первую модель – модель оценки функционирования процесса, для чего рассмотрим измерение и оценивание атрибутов и формирование оценки процессов обеспечения ИБ с помощью этой модели.

Каждый процесс характеризуется назначением (вход), результатом (выход), управляющими воздействиями и ресурсами.

Состояние любого процесса отображается совокупностью атрибутов мероприятий процесса, входных атрибутов, атрибутов управления, атрибутов ресурсов и выходных атрибутов:

$$Y = \langle Y_M, Y_{ВХ}, Y_У, Y_Р, Y_{ВЫХ} \rangle.$$

Для проведения оценки функционирования процессов каждый процесс должен быть представлен совокупностью атрибутов, требуемых для функционирования процессов в соответствии с их назначением:

$$Y^{ТР} = \langle Y_M^{ТР}, Y_{ВХ}^{ТР}, Y_У^{ТР}, Y_Р^{ТР}, Y_{ВЫХ}^{ТР} \rangle.$$

В общем случае каждый вид атрибута описывается набором атрибутов, т. е

$$Y^{TP} = \left\langle Y_{Mi}^{TP} \right\rangle, i = \overline{1,m_1}; Y_{BX}^{TP} = \left\langle Y_{BXi}^{TP} \right\rangle, i = \overline{1,m_2} \text{ и т.д.}$$

Для описания соответствия реальных атрибутов процесса требуемым атрибутам Y^{TP} формально введем числовую функцию на множестве атрибутов процесса $\rho = \rho (Y(u), Y^{TP})$, которая называется функцией соответствия. Каждый атрибут процесса измеряется с помощью функции соответствия. Конкретный вид функции зависит от метода измерения атрибута.

Для совокупности атрибутов функция соответствия $\rho (Y(u), Y^{TP})$ показывает степень достижения требуемых атрибутов. Совокупность атрибутов Y может быть случайной переменной $Y(u)$ (числовой или нечисловой), зависящей от стратегии $u \in U$. Стратегиями U могут быть следующие действия в отношении процессов обеспечения ИБ: применение базовой оценки рисков ИБ, использование определенного поставщика для реализации СОИБ, применение аутсорсинга для реализации некоторых процессов. Функция соответствия $\rho (Y(u), Y^{TP})$ в этом случае также может быть случайной величиной. Тогда показатель функционирования определяется математическим ожиданием функции соответствия:

$$W(u) = M\left[\rho\left(Y(u), Y^{TP}\right)\right].$$

Если $Y(u)$, и Y^{TP} – неслучайные переменные, то $W(u) = \rho (Y(u), Y^{TP})$.

На рис. 60 показана модель оценки процессов обеспечения ИБ организации на основе измерения атрибутов процессов.

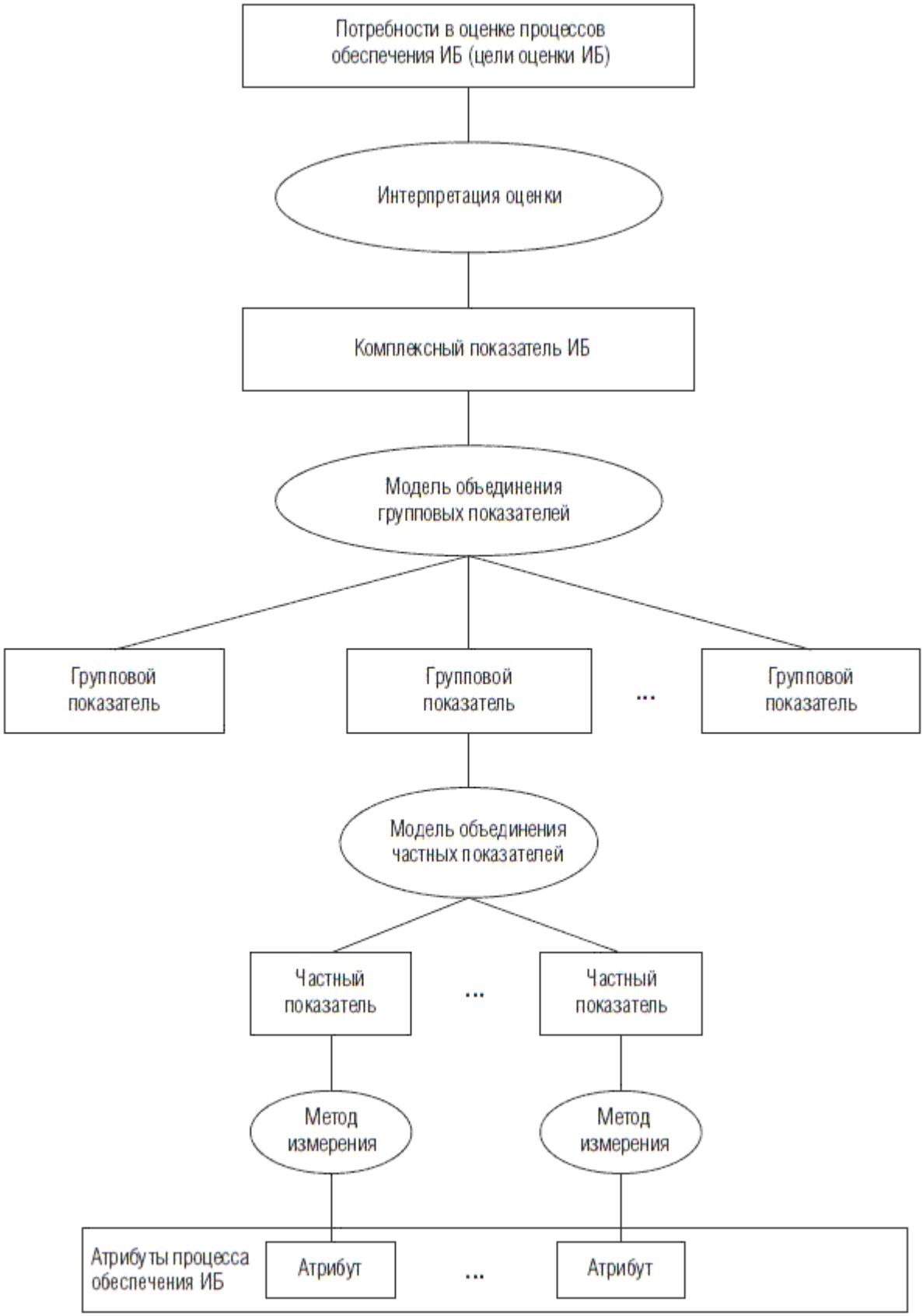


Рис. 60. Модель оценки процессов обеспечения ИБ организации

Данная модель оценки соответствия ИБ связывает потребности в оценке функционирования процессов обеспечения ИБ с соответствующими процессами и представляющими интерес атрибутами процессов. С помощью метода измерения атрибуты преобразовываются в основные меры (частные показатели), с помощью производных мер

формируются групповые показатели.

Примеры метрик из [30] и [23] для измерения атрибутов представлены в приложении 3

Для оценивания функционирования (правильности реализации) любого процесса введем групповой (векторный) показатель функционирования

$$W = \left\| W_{ВХ}, W_{У}, W_{Р}, W_{М}, W_{ВЫХ} \right\|,$$

объединяющий частные показатели разных видов:

– частные показатели правильности реализации входных атрибутов

$$W_{ВХ} = \rho\left(Y_{ВХ}, Y_{ВХ}^{ТР}\right);$$

– частные показатели правильности реализации атрибутов управления

$$W_{У} = \rho\left(Y_{У}, Y_{У}^{ТР}\right);$$

– частные показатели правильности реализации атрибутов ресурсов

$$W_{Р} = \rho\left(Y_{Р}, Y_{Р}^{ТР}\right);$$

– частные показатели правильности реализации атрибутов мероприятий

$$W_{М} = \rho\left(Y_{М}, Y_{М}^{ТР}\right);$$

– частные показатели правильности реализации выходных атрибутов

$$W_{ВЫХ} = \rho\left(Y_{ВЫХ}, Y_{ВЫХ}^{ТР}\right).$$

Для каждого атрибута процесса, когда Y (u), и $Y^{ТР}$ – неслучайные (детерминированные) переменные, функция соответствия служит частным показателем функционирования:

$$W_i = \rho_i\left(y_i, y_i^{ТР}\right), i = \overline{1, m_K},$$

где m_k – число атрибутов определенного вида, k = 5.

Введение векторного показателя функционирования накладывает дополнительные требования: минимальность числа частных показателей и полнота. Требование минимальности числа частных показателей связано со стремлением к снижению трудоемкости оценивания, однако при сохранении полноты охвата атрибутов процесса.

В зависимости от вида функции соответствия можно получить различные значения частных показателей функционирования. Вид функции соответствия определяется преобразованиями, которые допустимы в выбранных для метода измерения шкалах.

Например, пусть событие A означает достижение атрибута процесса требуемого значения. Вероятность P_u (A) наступления этого события зависит от стратегии $u \in U$. Тогда функция соответствия ρ в этом случае вводится как переменная, которая может принять лишь два значения 0 или 1, т. е.

$$\rho\left(y(u), y^{ТР}\right) = \begin{cases} 1, \text{если событие А наступило;} \\ 0, \text{в противном случае.} \end{cases}$$

Частные показатели могут иметь различную размерность. Поэтому при формировании группового показателя необходимо оперировать с нормированными значениями показателей.

Характеристики и свойства процессов обеспечения ИБ, которые несут атрибуты, не равнозначные с точки зрения реализации этих процессов. Поэтому необходимо определить способ объединения частных показателей (рис. 60) при формировании групповых показателей из частных. Наиболее часто применяемой производной мерой является усреднение объединяемых основных мер, т. е. групповые показатели формируются путем усреднения частных показателей, предполагая их равную значимость:

$$W_j = \frac{1}{n}\sum_{i=1}^{n} W_{ji},$$

где W_j – групповой показатель j -го процесса;

W_{ji} – частный показатель i- го атрибута j -го процесса;

n – число показателей всех измеряемых атрибутов j -го процесса.

Вычисление среднего значения для количественных показателей или вычисление медианы для качественных показателей дают хорошие результаты с точки зрения понимания правильности реализации процессов, однако адекватность такой обобщенной оценки не столь высока ввиду различной значимости оцениваемых атрибутов. Повысить адекватность обобщенной оценки процессов позволяет использование коэффициентов значимости (весовых коэффициентов) частных показателей.

Под значимостью частного показателя будем понимать важность оцениваемых частным показателем атрибутов процессов обеспечения ИБ с точки зрения функционирования (правильности реализации) этих процессов.

Групповые показатели при различной значимости частных показателей вычисляются следующим образом:

$$W_j = \frac{1}{n}\sum_{i=1}^{n} \alpha_{ji} W_{ji},$$

где α_{ji} – коэффициент значимости частного показателя i -го атрибута j -го процесса.

Значимость атрибутов процессов обеспечения ИБ может быть определена с помощью экспертных методов (непосредственной численной оценки, балльного оценивания, относительных частот рангов), основанных на субъективной оценке значимости экспертами, и аналитических методов с использованием формализованных процедур, снижающих субъективность оценки. Экспертные методы просты, субъективны. Аналитические методы менее субъективны, но сложны. Кроме того, они не ориентированы на процессный подход к оценке.

Комплексный показатель оценки ИБ (рис. 60) формируется как производная мера, объединяющая групповые показатели. Модель объединения групповых показателей может быть такой же, как модель объединения частных показателей, но со своими коэффициентами значимости. Другим вариантом модели объединения может быть модель предпочтения, когда значение комплексного показателя определяется по самому низкому значению показателя среди наиболее значимых групповых показателей.

3.3.2. Оценка информационной безопасности на основе модели зрелости процессов

Рассмотрим применение оценки возможности (оценки зрелости) процессов для оценки ИБ организации.

В ISO/IEC 15504 [29] определена модель оценки зрелости, основу которой составляют идентифицированные атрибуты оцениваемых процессов, представляющие измеримые характеристики возможностей того или иного процесса, и методы их оценивания.

Стандартом определена следующая шкала рейтингов оценки процесса, определяющих степень достижения определенных значений для оцениваемого атрибута процесса:

– N – не достигнуто: мало или нет свидетельств достижения определенным атрибутом оцениваемого процесса некоторого желаемого значения;

– P – частично достигнуто: существуют некоторые свидетельства приближения к желаемому значению определенного атрибута оцениваемого процесса;

– L – в значительной степени достигнуто: существуют свидетельства систематического приближения к определенному значению атрибута оцениваемого процесса, в оцениваемом

процессе могут существовать некоторые слабые места, связанные с этим атрибутом;

– F – полностью достигнуто: существуют свидетельства полного и систематического приближения к определенному значению атрибута оцениваемого процесса, никаких слабых мест, связанных с этим атрибутом, в оцениваемом процессе не существует.

Фактически рассматриваются определенные показатели атрибутов процессов, которые ранжируются по 4-уровневой шкале оценивания. Значения для оцениваемых параметров следующие:

– N – не достигнуто – от 0 до 15 %;

– P – частично достигнуто – от >15 до 50 %;

– L – в значительной степени достигнуто – от >50 до 85 %;

– F – полностью достигнуто – от >85 до 100 %.

При этом любая интересующая задача, представленная в спецификации процессного подхода с выделенными атрибутами данного процесса и установленным методом измерения данных атрибутов, может быть далее оценена на основе следующей обобщенной модели зрелости (уровням возможностей – рейтингам) процесса как представлено в таблице 10.

Таблица 10

Модель зрелости процессов

Шкала	Атрибуты процесса	Рейтинг
Уровень 1	Функционирование процесса	В значительной степени или полностью
Уровень 2	Функционирование процесса Менеджмент функционирования Менеджмент рабочего продукта	Полностью В значительной степени или полностью В значительной степени или полностью
Уровень 3	Функционирование процесса Менеджмент функционирования Менеджмент рабочего продукта Формализация процесса Развертывание процесса	Полностью Полностью Полностью В значительной степени или полностью В значительной степени или полностью
Уровень 4	Функционирование процесса Менеджмент функционирования Менеджмент рабочего продукта Формализация процесса Развертывание процесса Количественная оценка процесса Контроль процесса	Полностью Полностью Полностью Полностью Полностью В значительной степени или полностью В значительной степени или полностью
Уровень 5	Функционирование процесса Менеджмент функционирования Менеджмент рабочего продукта Формализация процесса Развертывание процесса Количественная оценка процесса Контроль процесса Инновация процесса Оптимизация процесса	Полностью Полностью Полностью Полностью Полностью Полностью Полностью В значительной степени или полностью В значительной степени или полностью

Для целей определения рейтинга (уровня) зрелости процесса выделяются характеризующие его атрибуты, которые можно было бы измерить, по следующим позициям:

– функционирование процесса – процесс выполняется и формирует определенные результаты;

– менеджмент функционирования – процесс управляем в контексте его назначения и целей процесса;

– менеджмент рабочего продукта – осуществляется управление результатами процесса в части их содержания и потребностей использования;

– формализация процесса – имеется полная формальная модель процесса, и его реализация осуществляется в соответствии со спецификацией;

– развертывание процесса – реализацией процесса охвачены все вовлеченные стороны;

– количественная оценка процесса – определены и используются количественные метрики процесса;

– контроль процесса – процесс контролируется во всех составляющих его работах и операциях;

– инновация процесса – разрабатываются и внедряются передовые технологии для работ и операций процесса;

– оптимизация процесса – осуществляются меры по улучшению процесса, результаты которых оцениваемы в количественном или качественном выражении.

Для оценки ИБ на основе модели зрелости необходимы два основных источника:

– требования к составу процессов менеджмента ИБ организации – требования ГОСТ Р ИСО / МЭК 27001;

– эталонная модель зрелости процессов ИБ.

Для идентифицированных процессов обеспечения ИБ должны быть разработаны:

– описание каждого из процессов в терминах уровней зрелости эталонной модели;

– методика оценки зрелости процессов, включающая анкеты для оценки возможностей процессов, в соответствии с заявленным уровнем зрелости.

С учетом анализа содержания и семантики требований ГОСТ Р ИСО/МЭК 27001 можно выделить следующие 17 процессов СМИБ организации:

– определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ;

– анализ и оценка рисков ИБ, варианты обработки рисков ИБ;

– определение/уточнение политики для СМИБ организации;

– выбор/уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;

– принятие руководством организации остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ;

– разработка плана обработки рисков ИБ;

– реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ;

– реализация программ по обучению и осведомленности ИБ;

– обнаружение и реагирование на инциденты безопасности ИБ;

– мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ;

– анализ эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ;

– внутренний аудит СМИБ;

– анализ СМИБ со стороны высшего руководства;

– реализация тактических улучшений в СМИБ, осуществляемых в рамках полномочий служб (ответственных) ИБ организации;

– реализация стратегических улучшений СМИБ, требующих принятия решений на

уровне руководства организации и инициирования процессов планирования СМИБ; использование опыта;

– информирование об изменениях и их согласование с заинтересованными сторонами;

– оценка достижения поставленных целей и потребностей в развитии СМИБ.

В [31] рассмотрен пример описания модели зрелости процесса ***«Анализ и оценка рисков ИБ, варианты минимизации рисков ИБ»,*** который приведен ниже.

Для процесса ***«Анализ и оценка рисков ИБ, варианты минимизации рисков ИБ»*** 4.2.1 c)÷f) СМИБ организации, определенной требованиями пунктами ГОСТ Р ИСО/МЭК 27001, описание модели его зрелости может быть определено следующим образом (приведем в качестве примера фрагменты описания нулевого, первого, третьего и пятого уровней зрелости процесса).

Модель зрелости

0-й уровень

На данном уровне наблюдается ***полное отсутствие определенного процесса*** *по анализу и оценке рисков ИБ.*

Не проводится оценка рисков ИБ для проектов, разрабатываемых стратегий и решений. Руководство организации не осознает возможных последствий для бизнеса организации, связанные с реализациями угроз ИБ, в спектре рисков организации не рассматриваются риски ИБ…

1-й уровень

В организации ***существуют документально зафиксированные*** *свидетельства осознания руководством существования проблем обеспечения ИБ. В частности, определена и документально зафиксирована область действия СМИБ.*

Информационные активы определены, составлен перечень их уязвимостей и вероятности использования уязвимостей угрозами. Просчитан ущерб от возможной реализации угроз, а также определены оценки актуальности угроз.

Процесс *анализа и оценки рисков как таковой* ***нестандартизирован.*** *Деятельности в рамках процесса оценки и анализа рисков применяются эпизодически и бессистемно. Создана, но не обновляется база инцидентов ИБ. Определены приоритеты рисков, но данные приоритеты учитывают не все инциденты ИБ…*

3-й уровень

Существует политика организации, в которой определяется периодичность и область оценки рисков ИБ. ***Процесс оценки рисков документирован и стандартизирован,*** *суть процесса доводится до заинтересованного персонала посредством обучения базовым принципам безопасности, оценки и анализа рисков ИБ. Разработан план работ по оценке рисков. Методология оценки рисков с большой степенью вероятности гарантирует, что основные риски ИБ будут выявлены, поскольку результаты деятельности в рамках процесса по оценке и анализу рисков согласованы с соответствующими политиками, стандартами и /или процедурами…*

5-й уровень

Оценка рисков в организации доведена до уровня лучших практик по оценке и анализу риска. ***Выбранная стратегия оценки рисков непрерывно совершенствуется,*** *ориентируясь на последние достижения в области ИБ, действующие международные стандарты и результаты сравнения с уровнем других организаций. Привлекаются сторонние сертифицированные эксперты для консультаций по вопросам рисков, оптимизации существующей системы сбора и анализа первичной информации для анализа рисков. Проводятся совещания по принципу «мозгового штурма» с целью выявить и проанализировать причины идентифицированных рисков. Система защитных мер строго скоординирована с приоритетами рисков и зависимостью «эффективность защитных мер – стоимость», комплексно используется установленная форма отчетности об эффективности защитных мер…*

По образу и подобию модель зрелости представляется для всех других процессов СМИБ организации.

Оценка уровня зрелости рассмотренного процесса ***«Анализ и оценка рисков ИБ, варианты минимизации рисков ИБ»*** СМИБ организации должна осуществлять на основе свидетельств выполненной деятельности по направлениям, соответствующим заявляемому или ожидаемому уровню зрелости. Например, для оценок на первый или третий уровень зрелости должны быть представлены свидетельства по следующим направлениям.

1-й уровень зрелости (начальный)

Вопрос	
Существует ли политика организации, в которой определена и документально зафиксирована область действия СМИБ организации?	
Существует ли документально зафиксированные свидетельства работ по оценке рисков ИБ в организации (стратегия оценки рисков, выбранный подход и т. п.)?	
Определены ли роли в рамках деятельности по оценке и обработке рисков ИБ?	
Выполнены ли идентификация информационных активов и их уязвимостей?	
Выполнена ли оценка потенциального ущерба бизнесу организации в случае реализации угроз ИБ?..	

3-й уровень зрелости

1) Процесс аттестован на соответствие 2-му уровню зрелости.

2) Получены свидетельства следующих действий.

Вопрос	
Определена ли периодичность и область оценки рисков в политике ИБ организации?	
Доведена ли данная политика до сведения всего персонала?	
Согласованы ли результаты деятельности в рамках процесса по оценке и анализу рисков с соответствующими политиками, стандартами и /или процедурами?	
Придерживается ли организация документированных планов, политик, стандартов и процедур по оценке и анализу рисков?	
Существует ли план работы в рамках процесса анализа и оценки рисков ИБ?	
Оценена ли возможность переноса информационных рисков на другие стороны (например, страховщиков, поставщиков, органы сертификации и т. п.)?..	

3.4. Риск-ориентированная оценка информационной безопасности

Оценка, основанная на оценке риска и оценке управления риском, отличается от системно-ориентированной и процессно-ориентированной оценки и называется [32] риск-ориентированной оценкой. Ключевое отличие риск-ориентированной оценки в том, что оценка должна быть направлена на анализ того, как менеджмент организации оценивает риски, контролирует и проверяет процессы менеджмента риска.

Риск-ориентированная оценка дает объективное и наиболее информативное представление об уровне эффективности деятельности организации, эффективности принимаемых менеджментом решений и эффективности затрат на поддержание и развитие бизнеса, исходя из сопоставления существующих рисков деятельности организации и принимаемых организацией мер по обработке таких рисков.

Целью риск-ориентированной оценки является определение, что:

– процессы менеджмента риска должным образом созданы и внедрены;

– процессы менеджмента риска, которые высшее руководство применяло в организации (процессы менеджмента риска на корпоративном уровне, уровне отдела,

подразделения, уровне бизнес-процесса), действуют надлежащим образом;

– в отношении рисков, подлежащих обработке, действия руководства организации направлены на снижение этих рисков до приемлемого уровня.

Алгоритм проведения риск-ориентированной оценки показан на рис. 61.

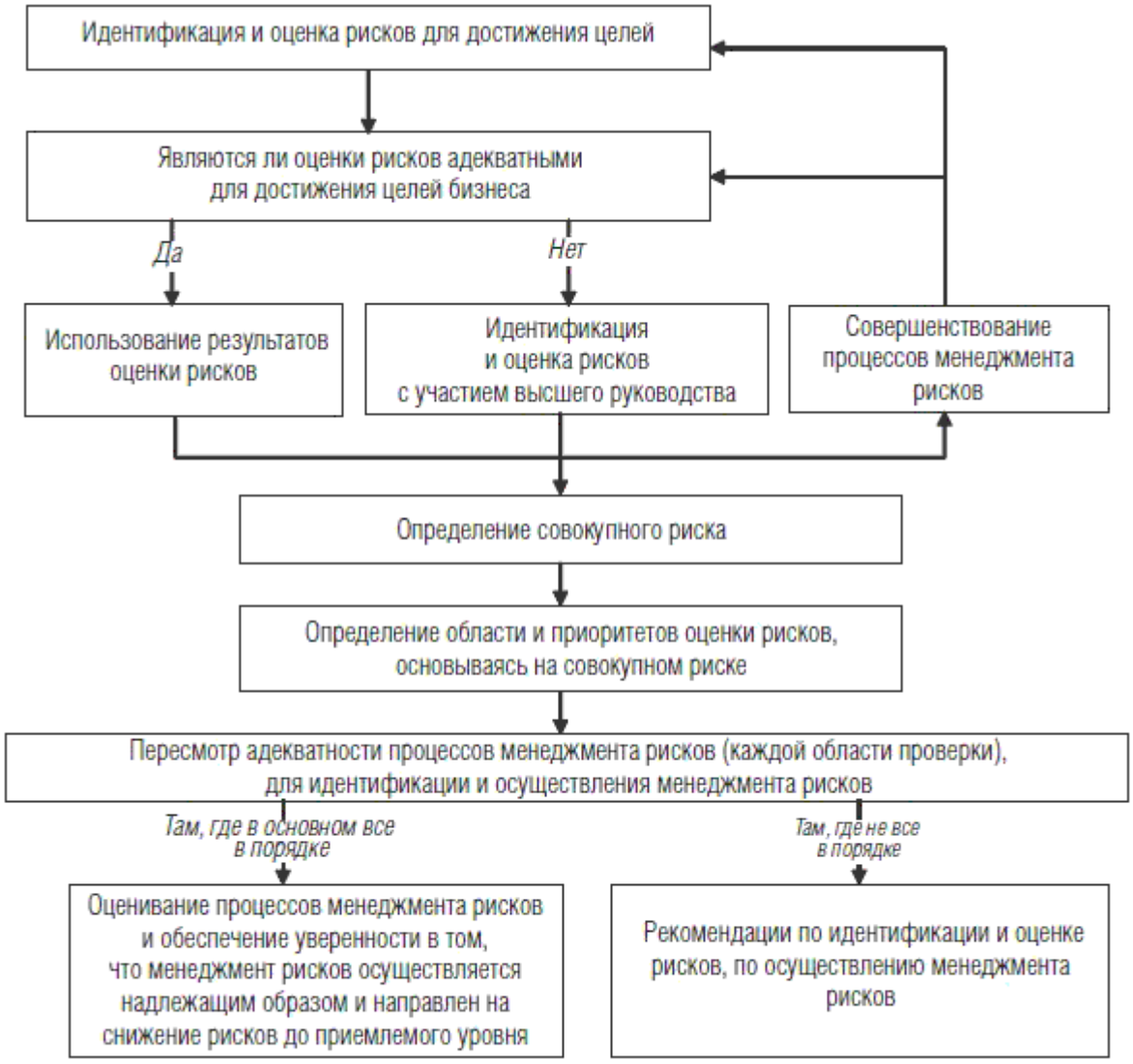


Рис. 61. Алгоритм проведения риск-ориентированной оценки

При проведении риск-ориентированной оценки следует:

– оценить инфраструктуру менеджмента риска, например ресурсов, документации, методов, сообщения;

– оценить специфические риски;

– при необходимости пересматривать бизнес-цели и процессы менеджмента риска;

– там, где нельзя считать процессы менеджмента риска адекватными существующим рискам, оценщик должен проводить собственную оценку риска (совместно с высшим руководством) для того, чтобы идентифицировать и оценить риски, а затем сконцентрироваться на том, что деятельности, связанные с менеджментом риска, выполняются надлежащим образом;

– конечный результат оценки должен заключаться в обеспечении уверенности в том, что менеджмент риска осуществляется надлежащим образом и направлен на снижение рисков до приемлемого уровня.

На рис. 62 показана модель риск-ориентированной оценки ИБ организации.

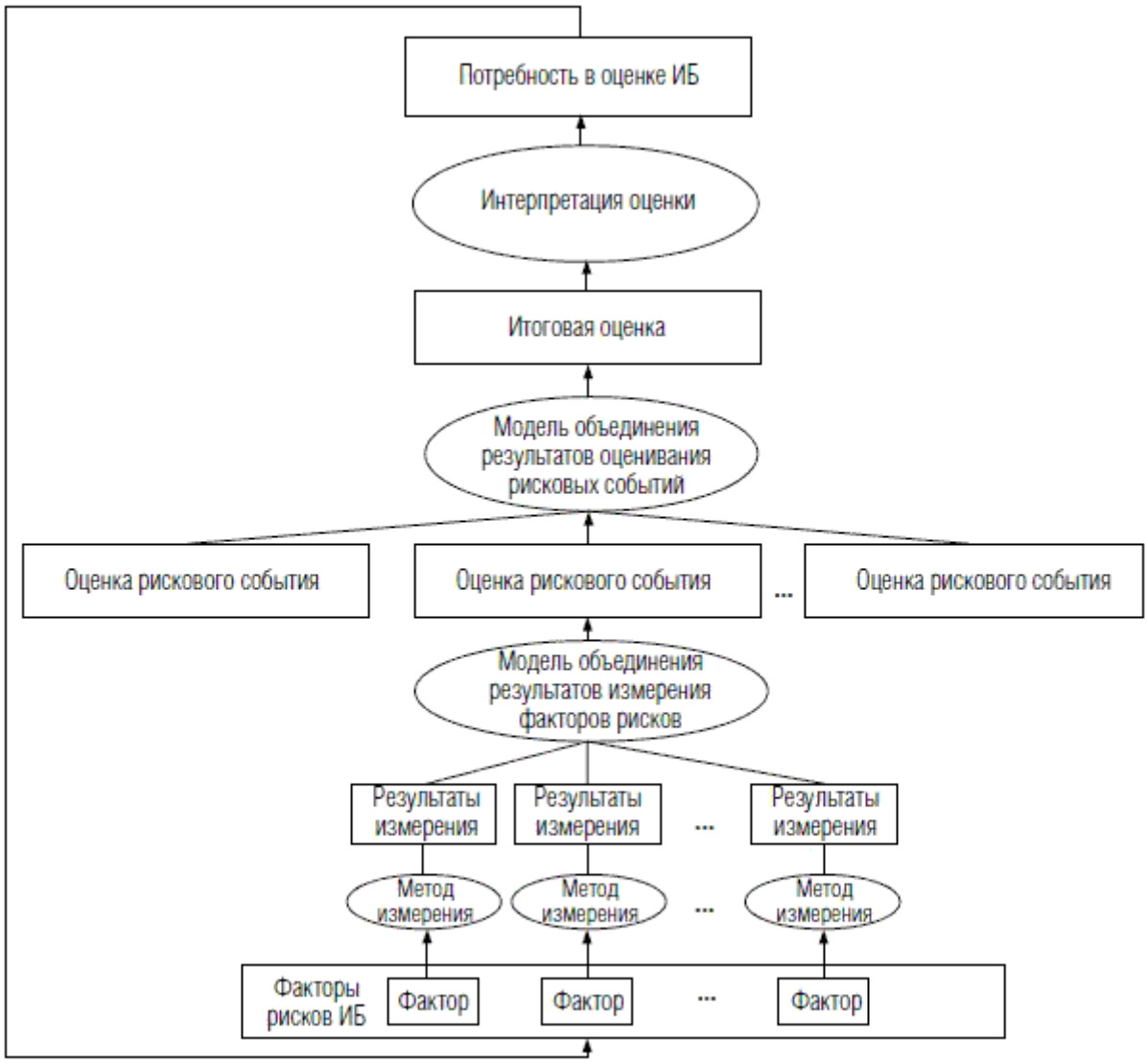


Рис. 62. Модель риск-ориентированной оценки ИБ организации

Риск реализуется через рисковые события, создающие ущерб целям бизнеса. В свою очередь, рисковые события являются следствием сочетания факторов риска, т. е. любому рисковому событию соответствует некоторый набор факторов риска.

Измерить фактор риска – это значит установить степень соответствия состояния фактора риска некоторому состоянию r^m, определяющему проявление рискового события.

Для совокупности факторов риска функция соответствия показывает

$$\rho = \rho\ (R, R^m)$$

степень достижения состояний факторов риска нежелательных состояний (состояний проявления рискового события).

Для каждого фактора риска, когда и являются неслучайными (детерминированными) переменными, функция соответствия служит результатом W_{ij} измерения, полученного с помощью выбранного метода измерения:

$$W_{ij} = \rho_{ij}\left(r_{ij}, r_{ij}^m\right),$$

где i – количество оцениваемых рисковых событий,

j – количество факторов риска i-го рискового события.

Объединение результатов измерения факторов риска с целью оценивания совокупности факторов риска может быть реализовано на основании модели предпочтения на множестве факторов риска, относящихся к каждому рисковому событию. Такой же подход может

применяться и для формирования итоговой оценки, определяющей совокупный риск ИБ организации.

Интерпретация оценки рисков ИБ и анализ достижения цели оценки (удовлетворения потребности) рисков ИБ завершают первый этап риск-ориентированной оценки. В соответствии с рис. 61 следующим шагом является этап оценки процессов менеджмента риска. Такая оценка может быть проведена на основании моделей оценки процессов, представленных в разделе 3.3.

4. Проблема персонала в задачах обеспечения информационной безопасности бизнеса

4.1. Общие сведения

4.1.1. Тенденции

Угрозы целям любого человеческого сообщества, исходящие от его участников, нельзя отнести к новым, появившимся в последнее время формам угроз. Такие угрозы существовали и реализовывались всегда, всегда осознавались и учитывались членами любого сообщества. Их изначальная природа погружена в сферу личностных мотивов, а также человеческих отношений [33] и не меняется многие тысячи лет. Глубинные причины внутренних происшествий в современной коммерческой организации совпадают с причинами внутренних происшествий в любом другом сообществе в истории человечества: в племени, в военном отряде, в монашеском ордене, в команде корабля.

В то же время среда существования человека и человеческих сообществ постоянно меняется в различных аспектах: социальном, культурном, экономическом, информационном. Не меняя природу человека, такие изменения среды тем не менее существенно воздействуют на пространство угроз в информационной сфере (угроз ИБ), в котором современная организация существует, пытаясь выжить и реализовать поставленные цели.

Среди наиболее важных (с точки зрения угроз ИБ от персонала) характеристик и явлений, которые присущи среде организации XXI в., отметим:

– высокий уровень конкуренции между предприятиями;

– изменчивость законодательных требований, в частности появление законодательных требований относительно обработки персональных данных, изменение норм трудового законодательства;

– открытость рынков, на которых информация имеет ключевое значение для выживания предприятия;

– высокая динамичность предприятий (быстрый рост небольших предприятий, изменчивость крупных), усложнение бизнес-процессов и изменчивость бизнес-целей;

– большой размер организационных структур и масштабов их деятельности;

– изменение трудовой культуры, текучесть кадров;

– высокие, постоянно растущие материальные ожидания персонала;

– социальная напряженность в обществе, «падение нравов»;

– уход документооборота и других операций в электронную форму;

– автоматизация деятельности, возрастание зависимости бизнеса от ИТ-услуг и качественных характеристик используемой информации, возрастание количества точек отказа, расположенных в информационных системах;

– возрастание сложности информационных технологий как в результате реагирования на усложнение деятельности организации, так и из-за существующих тенденций развития ИТ;

– высокая изменчивость ИТ как в результате реагирования на потребности бизнеса, так и из-за существующих тенденций развития ИТ;

– расширение каналов связи между информационными системами предприятий и сетью Интернет;

– расширение телекоммуникационных возможностей;

– повышение законодательных требований к объемным и качественным характеристикам отчетности, усиление ответственности организаций за качественных характеристики формируемой отчетности;

– масштабное использования аутсорсинга – использования услуг внешних организаций для решения задач, которые традиционно решались внутри организации ее работниками (бухгалтерских задач, задач разработки, внедрения и эксплуатации ИТ, задач аудита и др.).

Действие комплекса перечисленных взаимосвязанных явлений приводит к следующим последствиям:

1) информационная сфера организации стала более чувствительной для целей организации, цена успехов и неудач сильно возросла;

2) современные информационные технологии стали общедоступным для каждого сотрудника современной организации инструментом и неотъемлемым элементом многих видов основной, вспомогательной и управленческой деятельности, осуществляемых в организации; намеренное или случайное применение ИТ против целей организации может нанести организации существенный ущерб;

3) проблема доверия между организацией и ее сотрудниками становится год от года только острее.

В результате значимость угроз ИБ от персонала для современной организации постоянно возрастает.

В настоящей главе рассматриваются только преднамеренные угрозы ИБ от персонала, т. е. угрозы в информационной сфере организации, связанные с преднамеренными действиями ее персонала, осуществляемыми с использованием служебных полномочий и направленными против интересов организации.

4.1.2. Термины и определения

К сожалению, в современных источниках не существует устоявшейся терминологии в области угроз от персонала. Активно применяются термины: внутренний нарушитель, внутренний злоумышленник, инсайдер, корпоративное мошенничество, злоупотребление полномочиями и др. При этом содержание самих терминов часто неоднозначно даже у одного автора. Например, под инсайдером может пониматься:

– любой человек внутри организации;

– лицо, обладающее внутренней информацией организации, недоступной посторонним;

– лицо, нарушающее требования безопасности организации (например, «любой авторизованный пользователь, совершающий неразрешенные действия» [34]);

– лицо, обладающее правом принятия решений в организации (например, «физические лица, способные воздействовать на принятие решения о выдаче кредита банком» [35]);

– любое лицо, которому разрешен или был разрешен доступ к информационной системе [36];

– злонамеренный сотрудник организации, внутренний злоумышленник (например, «лица, которым разрешено или было разрешено использовать информационные системы, которые они в конечном счете использовали для совершения преступления (или нанесения ущерба)» [37]);

– сотрудник организации, пользующийся служебными полномочиями в личных целях.

Перечисленные категории близки, но не совпадают полностью, что создает неопределенность, препятствующую накоплению знаний в рассматриваемой области и

обмену знаниями между специалистами.

Поэтому в настоящей главе мы ограничили ряд необходимых для изложения материала терминов, а их содержание раскрыли в данном подразделе.

Сотрудник организации – лицо, выполняющее работу в этой организации на временной или постоянной основе, которому организация доверяет, предоставляя необходимые ему для выполнения обязанностей полномочия и информацию.

Персонал организации – множество всех сотрудников организации.

Инсайдер – лицо, обладающее служебными полномочиями в отношении информационных активов организации и (или) знаниями особенностей ИТ-среды организации, которые могут быть использованы нежелательным для организации образом.

К служебным полномочиям инсайдера могут быть отнесены следующие:

– доступ к служебной информации ограниченного распространения, представленной в различной форме (например, персональные данные, информация, составляющая коммерческую и банковскую тайны);

– полномочия в рамках корпоративного управления (руководство, планирование, координация, контроль, согласование, инициативы по внесению изменений, ознакомление с документами, обеспечение и др.);

– доступ к информационным системам организации на различных уровнях: на уровне аппаратного обеспечения, на уровне операционной системы, на сетевом уровне, на уровне администрирования приложений и баз данных, на уровне пользователя приложений (доступ на уровне пользователя за исключением систем общего доступа, таких как публичный веб-сайт, банкоматы, терминалы платежной системы и т. п.);

– физический доступ на объекты организации (доступ к средствам обработки информации, съемным носителям информации и т. д.);

– использование телефонной, радио и других видов связи с терминалов на территории организации;

– другие полномочия.

Понятно, что большинство инсайдеров являются сотрудниками организации (относятся к персоналу организации). Однако отдельными характерными для инсайдера признаками могут обладать и другие лица:

– сотрудники регулирующих и правоохранительных органов, которым для выполнения их функций необходим доступ на территорию и (или) к информационной системе организации;

– сотрудники организаций-подрядчиков (в том числе потенциальных, с которыми еще не установлены договорные отношения);

– бывшие сотрудники организации, которые зачастую обладают серьезными знаниями внутренней среды организации и поддерживают контакты с бывшими коллегами;

– другие лица, которым правомерно (например, в силу деловой необходимости) организацией предоставлены характерные для инсайдера возможности (знания и (или) полномочия).

Далее в настоящей главе с целью упрощения будем рассматривать только умышленные (являющиеся результатом преднамеренных действий) ***угрозы ИБ от персонала*** организации (к персоналу относится большая часть инсайдеров). Однако в жизни все сложнее, и на практике необходимо учитывать опасности, исходящие от инсайдеров всех категорий.

Инцидентом с участием сотрудника организации ***(нападением, атакой)*** будем называть происшествие, в результате которого наступили (или с высокой вероятностью могли наступить) негативные последствия для организации и значимой причиной которого стало преднамеренное использование (или неиспользование – бездействие) сотрудником служебных полномочий и (или) знаний.

Происшествия, в которых негативная роль сотрудников связана с их непреднамеренными действиями (ошибками, халатностью, обманом со стороны третьих лиц), не будут рассматриваться в настоящей главе, хотя зачастую такие происшествия также представляют значительную опасность.

Злоумышленник – лицо, которое планирует, совершает или совершило заранее обдуманное действие, приводящее к негативным последствиям для организации. При этом злоумышленник предвидит и осознает опасные последствия своего действия (бездействия) или не предвидит и не осознает, хотя должно и может предвидеть и осознавать возможность наступления этих последствий.

Внутренний злоумышленник – лицо из числа сотрудников организации, которое планирует, совершает или совершило заранее обдуманное действие, приводящее к негативным последствиям для организации с использованием служебных полномочий и (или) знаний особенностей ИТ-среды организации.

Ошибка – неправильная оценка лицом, совершающим некоторое действие (бездействие), обстановки и (или) последствий своего действия (бездействия).

Фактор – объект, субъект или явление, которое имеет значение (оказывает влияние) в отношении некоторой интересующей нас цели.

Фактор риска ИБ от персонала – объект, субъект или явление, которое оказывает влияние на риски ИБ организации, связанные с персоналом.

4.1.3. Общая характеристика угроз

Далее приводятся некоторые утверждения, характеризующие угрозы ИБ от персонала.

Использование инсайдерами служебных полномочий и знаний ИТ-среды организации в интересах, противоречащих интересам организации, является одной из наиболее опасных по возможным негативным последствиям угроз ИБ организации.

Негативные последствия действий внутреннего злоумышленника могут быть не очевидны для менеджмента организации, поскольку могут проявиться спустя продолжительное время, заключаться в невозможности реализации долгосрочных целей организации, в снижении эффективности основных и вспомогательных видов деятельности, в финансовых потерях третьих лиц и т. д.

Внутренний злоумышленник будет использовать самое слабое звено системы защиты организации – и атака будет выполнена наиболее простым и безопасным из известных злоумышленнику способов. В частности, нападение внутреннего злоумышленника с большой вероятностью произойдет неожиданно для организации.

Внутренний злоумышленник будет управлять своими знаниями и знаниями окружающих его сотрудников в собственных интересах, воздействуя на информационную сферу организации.

Внутренний злоумышленник хорошо информирован о том способе атаки, который собирается использовать. Велика вероятность, что он воспользуется видами доступа, которые применяет повседневно в своей работе.

Различные угрозы ИБ от персонала не равновероятны между собой из-за того, что разным угрозам соответствуют разные мотивы, разные возможности их осуществления, различная привлекательность результата для злоумышленника.

Главной причиной возникновения угроз ИБ от персонала является возможность конфликта интересов – скрытого противоречия между служебными обязанностями сотрудника перед организацией и личными интересами сотрудника.

Сущностью угрозы ИБ от персонала является злоупотребление доверием организации, причем доверие организации проявляется в предоставлении инсайдеру полномочий в отношении информационных активов организации, а также возможности получения знаний об ИТ-среде организации.

Атака на информационные активы организации, совершаемая внутренним

злоумышленником, является элементом противоправной деятельности одного правонарушителя или группы правонарушителей. Деятельность внутреннего злоумышленника в ИТ-среде организации в различных случаях может составлять как значительную, так и небольшую часть общей схемы противоправной деятельности. Поэтому практически идентифицировать атаку, определить личность злоумышленника и действительную цель атаки во многих случаях возможно лишь путем вскрытия всей схемы противоправной деятельности.

Для большинства угроз ИБ от персонала характерна высокая скрытность действий внутреннего злоумышленника.

Меры разграничения и управления доступом к информационным активам организации прозрачны для инсайдеров, поскольку они обладают служебными полномочиями доступа, что определяет необходимость применения специализированных мер для противодействия угрозам ИБ от персонала.

Внутренний злоумышленник потенциально располагает значительными временными ресурсами для получения необходимых знаний, подготовки и проведения атаки.

Также для угроз ИБ от персонала характерна непредсказуемость последствий – негативные последствия самого разного характера и масштаба как для организации в целом, так и персональные последствия для ее сотрудников.

Практически нет такого умышленно вызванного происшествия, в котором его бенефициару не был бы выгоден «свой человек» в организации (для получения информации, подготовки, проведения, сокрытия следов, использования последствий).

Атаки, совершаемые внутренними злоумышленниками, могут быть однократными или длящимися. Следует считать высокой вероятность совершения повторных атак внутренним злоумышленником, успешно совершившим некоторую атаку.

Актуальность угроз ИБ от персонала обозначена в современных нормативных документах по ИБ, например в стандарте Банка России СТО БР ИББС – 1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [26]:

«Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности».

«Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает».

С точки зрения действующего законодательства действия внутренних злоумышленников, направленные против законных интересов организации, в зависимости от их конкретного содержания могут квалифицироваться как различные уголовные и административные правонарушения:

– кража (в соответствии со ст. 158 УК РФ);

– мошенничество (в соответствии со ст. 159 УК РФ);

– присвоение или растрата (в соответствии со ст. 160 УК РФ);

– причинение имущественного ущерба путем обмана или злоупотребления доверием (в соответствии со ст. 165 УК РФ);

– незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (в соответствии со ст. 183 УК РФ);

– злоупотребление полномочиями (в соответствии со ст. 201 УК РФ);

– коммерческий подкуп (в соответствии со ст. 204 УК РФ);

– неправомерный доступ к компьютерной информации (в соответствии со ст. 272 УК РФ);

– создание, использование и распространение вредоносных программ для ЭВМ (в соответствии со ст. 273 УК РФ);

– нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (в соответствии со ст. 274 УК РФ);

– разглашение информации с ограниченным доступом (в соответствии со ст. 13.14 АК РФ).

4.1.4. Примеры инцидентов

Общие сведения

В настоящем разделе приводятся описания опубликованных подробностей некоторых нашумевших инцидентов. При этом обобщение инцидентов дает целый букет обстоятельств, характеризующих разнообразие угроз ИБ от персонала как в части мотивов и условий, так и в части используемых средств. Среди наиболее часто происходящих происшествий отметим следующие:

– утечка служебной информации;

– кража клиентов и бизнеса организации;

– саботаж инфраструктуры;

– внутреннее мошенничество;

– фальсификация отчетности;

– торговля на рынках на основе инсайдерской, служебной информации;

– злоупотребление полномочиями.

Аннотация

В отместку за слишком маленькую премию 63-летний Рожер Дуронио (бывший системный администратор компании UBS Paine Webber) установил на серверах компании «логическую бомбу», которая уничтожила все данные и парализовала работу компании на продолжительное время.

Описание инцидента

Дуронио был недоволен своей зарплатой, составляющей 125 000 долларов в год, возможно, это и послужило причиной внедрения «логической бомбы». Однако последней каплей для системного администратора стала полученная им премия в размере 32 000 долларов вместо ожидаемых 50 000 долларов [38, 39]. Когда он обнаружил, что его премия гораздо меньше, чем он ожидал, Дуронио потребовал от начальства перезаключить трудовой договор на сумму 175 000 долларов в год, или же он покинет компанию. В повышении зарплаты ему было отказано, кроме того, его попросили покинуть здание банка. В отместку за такое обращение Дуронио решил воспользоваться своим «изобретением», внедренным заранее, предвидя такой поворот событий.

Внедрение «логической бомбы» Дуронио осуществил с домашнего компьютера за несколько месяцев до того, как получил слишком маленькую, на его взгляд, премию. «Логическая бомба» была установлена примерно на 1500 компьютеров в сети филиалов по всей стране и настроена на определенное время – 9.30, как раз на начало банковского дня [40].

Уволился Дуронио из UBS Paine Webber 22 февраля 2002 г., а четвертого марта 2002 г. «логическая бомба» последовательно удалила все файлы на главном сервере центральной базы данных и 2000 серверов в 400 филиалах банка, при этом отключив систему резервного копирования.

Адвокат Дуронио в течение судебного процесса указывал на то, что виновником происшедшего мог быть не один только обвиняемый: учитывая незащищенность ИТ-систем UBS Paine Webber, под логином Дуронио туда мог попасть и любой другой сотрудник. О проблемах с ИТ-безопасностью в банке стало известно еще в январе 2002 г.: при проверке установили, что 40 человек из ИТ-службы могли войти в систему и получить права администратора по одному и тому же паролю, и понять, кто именно совершил то или иное

действие, не представлялось возможным. Адвокат также выдвигал обвинения в адрес UBS Paine Webber и компании @Stake, нанятой банком для расследования случившегося, в уничтожении доказательств атаки. Однако неоспоримым доказательством вины Дуронио были найденные на его домашних компьютерах отрывки вредоносного кода, а в его шкафу – распечатанная копия кода.

Возможности инсайдера

Как на одного из системных администраторов компании на Дуронио была возложена ответственность за всю компьютерную сеть UBS PaineWebber, и, соответственно, он имел к ней доступ. У него также был доступ к сети со своего домашнего компьютера посредством безопасного интернет-соединения.

Причины

Как уже указывалось ранее, его мотивами были деньги и месть. Дуронио получил годовую зарплату 125 000 долларов и премию 32 000 долларов, в то время как ожидал 50 000 долларов, и таким образом отомстил за свое разочарование.

Кроме того, Дуронио решил заработать на атаке: ожидая падения акций банка в связи с ИТ-катастрофой, он сделал фьючерсную заявку на продажу, чтобы при снижении курса получить разницу. На это обвиняемый потратил 20 000 долларов. Однако бумаги банка не упали, а инвестиции Дуронио не окупились [39].

Последствия

Заложенная Дуронио «логическая бомба» остановила работу 2000 серверов в 400 офисах компании. По словам ИТ-менеджера UBS Paine Webber Эльвиры Марии Родригес (Elvira Maria Rodriguez), это была катастрофа «на 10 с плюсом по 10-балльной шкале». В компании воцарился хаос, который почти сутки устраняли 200 инженеров из IBM. Всего над исправлением ситуации работало около 400 специалистов, включая ИТ-службу самого банка. Ущерб от случившегося оценивают в 3,1 млн долларов. Восемь тысяч брокеров по всей стране вынуждены были прекратить работу. Некоторым из них удалось вернуться к нормальной деятельности через несколько дней, некоторым – через несколько недель, в зависимости от того, насколько сильно пострадали их базы данных и осуществлялось ли в филиале банка резервное копирование. В целом же банковские операции были возобновлены в течение нескольких дней, однако работа некоторых серверов так и не была восстановлена в полном объеме, в большей степени из-за того, что на 20 % серверов не было средств резервного копирования. Только через год весь серверный парк банка снова был полностью восстановлен.

При рассмотрении дела Дуронио в суде его обвиняли по следующим статьям:

– мошенничество с ценными бумагами – обвинение по данной статье влечет за собой максимальное наказание в виде лишения свободы на 10 лет в федеральной тюрьме и штрафа в размере 1 млн долларов;

– мошенничество в деятельности связанной с компьютерами – обвинение по данной статье влечет за собой максимальное наказание в виде лишения свободы на 10 лет и штрафа в размере 250 000 долларов [40].

В итоге судебного процесса в конце декабря 2006 г. Дуронио был осужден на 97 месяцев без права досрочного освобождения.

«Вымпелком» и «Шерлок»

Аннотация

С целью наживы бывшие сотрудники компании «Вымпелком» (торговая марка «Билайн») через веб-сайт предлагали детализацию телефонных переговоров сотовых операторов.

Описание инцидента

Сотрудники компании «Вымпелком» (бывшие и действующие) организовали в Интернете сайт www.sherlok.ru, о котором в компании «Вымпелком» узнали в июне 2004 г. [41]. Организаторами данного сайта предлагалась услуга – поиск людей по фамилии,

телефону и другим данным. В июле организаторы сайта предложили новую услугу – детализацию телефонных переговоров сотовых операторов. Детализация разговоров – это распечатка номеров всех входящих и исходящих звонков с указанием длительности разговоров и их стоимости, используемая операторами, например для выставления счетов абонентов. По этим данным можно сделать вывод о текущей деятельности абонента, его сфере интересов и круге знакомств. В пресс-релизе Управления «К» министерства внутренних дел (далее – МВД) уточняется, что такая информация стоила заказчику 500 долларов.

Сотрудники компании «Вымпелком», обнаружив данный сайт, самостоятельно собрали доказательства преступной деятельности сайта и передали дело в МВД. Сотрудники МВД возбудили уголовное дело и совместно с компанией «Вымпелком» установили личности организаторов данного преступного бизнеса. А 18 октября 2004 г. был задержан с поличным главный подозреваемый[1].

Кроме того, 26 ноября 2004 г. были задержаны остальные шестеро подозреваемых, в числе которых были трое сотрудников абонентской службы самой компании «Вымпелком». В ходе следствия выяснилось, что сайт был создан бывшим студентом Московского государственного университета, не работавшим в данной компании.

Делопроизводство по данному инциденту стало возможным благодаря вынесенному в 2003 г. определению Конституционного суда, признавшего, что в детализации вызовов содержится тайна телефонных переговоров, охраняемая законом.

Возможности инсайдера

Двое из числа выявленных среди участников инцидента сотрудников компании «Вымпелком» работали операционистами в компании, а третий являлся бывшим сотрудником и на момент преступления работал на Митинском рынке.

Работа в самой компании операционистами свидетельствует о том, что данные сотрудники имели непосредственной доступ к информации, предлагаемой к продаже на сайте www.sherlok.ru. Кроме того, так как бывший сотрудник компании уже работал на Митинском рынке, то можно предположить, что со временем одним из каналов сбыта данной информации или какой-либо еще информации из баз данных компании «Вымпелком» мог стать и данный рынок.

Последствия

Основными последствиями для компании «Вымпелком» от данного инцидента могли быть удар по репутации самой компании и потеря клиентов. Однако данный инцидент был предан огласке непосредственно благодаря активным действиям самой компании.

Кроме того, предание огласки данной информации могло негативным образом сказаться на клиентах компании «Вымпелком», так как детализация разговоров позволяет сделать вывод о текущей деятельности абонента, его сфере интересов и круге знакомств.

В марте 2005 г. Останкинский районный суд города Москва приговорил подозреваемых, в числе которых трое сотрудников компании «Вымпелком», к различным штрафам [42]. Так, организатор группы оштрафован на 93 000 рублей. Однако работа сайта www.sherlok.ru была прекращена на неопределенный срок только с 1 января 2008 г.

Крупнейшая утечка персональных данных за всю историю Японии

Аннотация

Летом 2006 г. произошла самая крупная утечка персональных данных за всю историю Японии: сотрудник полиграфического и электронного гиганта Dai Nippon Printing украл диск с приватными сведениями почти девяти миллионов граждан.

Описание инцидента

Японская фирма Dai Nippon Printing, специализирующаяся на выпуске

---

[1] Согласно ст. 138 («Нарушение тайны телефонных переговоров») и ст. 272 УК («Незаконный доступ к информации ЭВМ, их систем и сетей») ему грозило до 5 лет лишения свободы.

полиграфической продукции, допустила крупнейшую утечку в истории своей страны. Хирофуми Йокояма, бывший сотрудник одного из подрядчиков компании, скопировал на мобильный винчестер и украл персональные данные клиентов фирмы. В общей сложности под угрозу попали 8,64 млн человек, так как похищенная информация содержала имена, адреса, телефоны и номера кредитных карт. В похищенной информации содержались сведения о клиентах 43 различных компаний, например о 1 504 857 клиентах компании American Home Assurance, 581 293 клиентах компании Aeon Co и 439 222 клиентах NTT Finance [43, 44].

После похищения данной информации Хирофуми открыл торговлю приватными сведениями порциями от 100 000 записей. Благодаря стабильному доходу инсайдер даже покинул постоянное место работы. К моменту задержания Хирофуми успел продать данные 150 000 клиентов крупнейших кредитных фирм группе мошенников, специализирующихся на онлайн-покупках. Кроме того, часть данных уже была использована для мошенничества с кредитными картами.

Более половины организаций, данные клиентов которых были похищены, даже не были предупреждены об утечке информации.

Последствия

В результате данного инцидента убытки граждан, которые пострадали из-за мошенничества с кредитными картами, ставшего возможным только вследствие этой утечки, составили несколько миллионов долларов. Всего пострадали клиенты 43 различных компаний, в том числе Toyota Motor Corp., American Home Assurance, Aeon Co и NTT Finance. Однако более половины организаций даже не были предупреждены об утечке.

В 2003 г. в Японии был принят закон Personal Information Protection Act 2003 (PIPA), но прокуратура не смогла его применить в реальном судебном разбирательстве по данному делу в начале 2007 г. Обвинение не смогло инкриминировать инсайдеру нарушение закона PIPA. Его обвиняют лишь в краже винчестера стоимостью 200 долларов.

Не оценили. Запорожский хакер против украинского банка

Аннотация

Бывший системный администратор одного из крупных банков Украины перевел через банк, в котором раньше работал, со счета региональной таможни на счет несуществующей днепропетровской фирмы-банкрота около 5 млн гривен.

Описание инцидента

Карьера системного администратора началась после того, как он окончил техникум и был принят на работу в один из крупных банков Украины в отдел программного и технического обеспечения. Спустя некоторое время руководство заметило его талант и решило, что он больше принесет пользы банку в качестве начальника отдела. Однако приход нового руководства в банке повлек за собой и кадровые перестановки. Его попросили временно освободить занимаемую должность. Вскоре новое руководство начало формировать свою команду, а его талант оказался невостребованным, и ему предложили несуществующую должность заместителя начальника, но уже в другом отделе. В результате таких кадровых перестановок он стал заниматься совершенно не тем, в чем разбирался лучше всего.

Системный администратор не мог мириться с таким отношением руководства к себе и уволился по собственному желанию. Однако ему не давала покоя собственная гордость и обида на руководство, кроме того, ему хотелось доказать, что он лучший в своем деле, и вернуться в отдел с которого началась его карьера.

Уволившись, бывший системный администратор решил вернуть у бывшего руководства интерес к своей персоне посредством использования несовершенства применяемой практически во всех банках Украины системы «Банк-Клиент» [2]. План

[2] Данная система позволяет оперативно переводить денежные средства с одного расчетного счета клиентов на другой.

системного администратора состоял в том, что он решил разработать свою программу защиты и предложить ее банку, вернувшись на свое прежнее место работы. Реализация плана заключалась в проникновении в систему «Банк-Клиент» и внесении в нее минимальных изменений. Весь расчет был сделан на то, что в банке должны были обнаружить взлом системы.

Для проникновения в указанную систему бывший системный администратор воспользовался паролями и кодами, которые узнал еще в процессе работы с данной системой. Вся остальная информация, необходимая для взлома, была получена с различных хакерских сайтов, где в подробностях были расписаны различные случаи взломов компьютерных сетей, методики взлома и размещалось все необходимое для взлома программное обеспечение.

Создав в системе лазейку, бывший системный администратор периодически проникал в компьютерную систему банка и оставлял в ней различные знаки, пытаясь привлечь внимание к фактам взлома. Специалисты банка должны были обнаружить взлом и забить тревогу, но, к его удивлению, проникновения в систему никто даже не замечал.

Тогда системный администратор решил изменить свой план, внеся в него коррективы, которые бы не смогли остаться незамеченными. Он решил подделать платежное поручение и перевести по нему через компьютерную систему банка крупную сумму. С помощью ноутбука и мобильного телефона со встроенным модемом системный администратор около 30 раз проникал в компьютерную систему банка: просматривал документы, счета клиентов, движение денежных средств – в поисках подходящих клиентов. В качестве таких клиентов им были выбраны региональная таможня и днепропетровская фирма-банкрот [45, 46].

Получив в очередной раз доступ к системе банка, он создал платежное поручение, в котором с лицевого счета региональной таможни снял и перечислил через банк на счет фирмы-банкрота 5 млн гривен. Кроме того, им целенаправленно было сделано несколько ошибок в «платежке», что в свою очередь должно было еще больше способствовать привлечению внимания со стороны специалистов банка. Однако даже такие факты были не замечены специалистами банка, обслуживающими систему «Банк-Клиент», и они спокойно перечислили 5 млн гривен на счет уже не существующей фирмы.

В действительности системный администратор рассчитывал на то, что денежные средства не будут переведены, что факт взлома будет обнаружен до перевода средств, но на практике все оказалось по-другому и он стал преступником и его липовый перевод перерос в кражу.

Факт взлома и хищения денежных средств в особо крупных размерах были обнаружены только через несколько часов после перевода, когда работники банка позвонили на таможню – подтвердить перевод. Но там сообщили, что такую сумму никто не перечислял. Деньги в срочном порядке были возвращены назад в банк, а в прокуратуре Запорожской области заведено уголовное дело.

Последствия

Банк не понес никаких потерь, так как деньги были возвращены владельцу, а компьютерная система получила минимальные повреждения, вследствие чего руководство банка отказалось от каких-либо претензий в адрес бывшего системного администратора.

В 2004 г. указом президента Украины была усилена уголовная ответственность за компьютерные преступления: штрафы от 600 до 1000 не облагаемых налогом минимумов, лишение свободы – от 3 до 6 лет. Однако бывший системный администратор совершил преступление до вступления в силу указа президента.

В начале 2005 г. состоялся суд над системным администратором. Его обвинили в совершении преступления по части 2 статьи 361 Уголовного кодекса Украины – незаконное вмешательство в работу компьютерных систем с нанесением вреда и по части 5 статьи 185 – кража, совершенная в особо крупных размерах. Но так как руководство банка отказалось от

каких-либо претензий в его адрес, то статью за кражу с него сняли, а часть 2 статьи 361 поменяли на часть 1 – незаконное вмешательство в работу компьютерных систем.

Бесконтрольный трейдинг в банке Societe Generale

Аннотация

24 января 2008 г. Societe Generale объявил о потере 4,9 млрд евро из-за махинаций своего трейдера Жерома Кервьеля [47]. Как показало внутреннее расследование, в течение нескольких лет трейдер открывал сверхлимитные позиции на фьючерсы на европейские фондовые индексы. Общая сумма открытых позиций составила 50 млрд евро.

Описание инцидента

С июля 2006 по сентябрь 2007 г. компьютерная система внутреннего контроля 75 раз (именно столько раз Жером Кервьель осуществлял несанкционированные операции либо его позиции превышали допустимый лимит) выдавала предупреждение о возможных нарушениях. Сотрудники отдела мониторинга рисков банка не осуществляли детальных проверок по этим предупреждениям [48].

Впервые экспериментировать с неавторизованным трейдингом Кервьель начал уже в 2005 г. Тогда он занял короткую позицию на акции Allianz, ожидая падения рынка. Вскоре рынок действительно упал (после террористических акций в Лондоне), так были заработаны первые 500 000 евро. О своих чувствах, которые он испытал от своего первого успеха, Кервьель впоследствии рассказал следствию: «Я уже знал, как закрыть мою позицию, и был горд за полученный результат, но вместе с тем и удивлен. Успех заставил меня продолжать, это было как снежный ком… В июле 2007 г. я предложил занять короткую позицию в расчете на падение рынка, но не встретил поддержки со стороны своего руководителя. Мой прогноз оправдался, и мы получили прибыль, на этот раз она была вполне легальной. Впоследствии я продолжал проводить такого рода операции на рынке либо с согласия начальства, либо при отсутствии его явного возражения… К 31 декабря 2007 г. моя прибыль достигла 1,4 млрд евро. В тот момент я не знал, как объявить об этом моему банку, так как это была очень большая, нигде не задекларированная сумма. Я был счастлив и горд, но не знал, как объяснить своему руководству поступление этих денег и не навлечь на себя подозрение в проведении несанкционированных сделок. Поэтому решил скрыть мою прибыль и провести противоположную фиктивную операцию…» [49].

В действительности в начале января того же года Жером Кервьель вновь вступил в игру с фьючерсными контрактами на три индекса Euro Stoxx 50, DAX и FTSE, помогавшими ему обыгрывать рынок в конце 2007 г. (правда, тогда он предпочитал занимать короткую позицию). По подсчетам, в его портфеле накануне 11 января было 707, 9 тыс. фьючерсов (каждый стоимостью по 42,4 тыс. евро) на Euro Stoxx 50, 93,3 тыс. фьючерсов (192,8 тыс. евро за 1 штуку) на DAX и 24,2 тыс. фьючерсов (82,7 тыс. евро за 1 контракт) на индекс FTSE. В целом спекулятивная позиция Кервьеля равнялась 50 млрд евро, т. е. была больше стоимости банка, в котором он работал [49].

Зная время проверок, он в нужный момент открывал фиктивную хеджирующую позицию, которую позже закрывал. В результате проверяющие никогда не видели ни одной позиции, которую можно было назвать рискованной. Их не могли насторожить и крупные суммы сделок, которые вполне обычны для рынка фьючерсных контрактов по индексам. Подвели его фиктивные сделки, проводимые со счетов клиентов банка. Использование счетов различных клиентов банка не приводило к видимым для контролеров проблемам. Однако по истечении определенного времени Кервьель начал использовать счета одних и тех же клиентов, что привело к «ненормальной» активности, наблюдаемой за данными счетами, и, в свою очередь, привлекло внимание контролеров [50]. Это стало концом аферы. Выяснилось, что партнером Кервьеля по мультимиллиардной сделке был крупный немецкий банк, якобы подтвердивший астрономическую транзакцию по электронной почте. Однако электронное подтверждение вызвало у проверяющих подозрения, для проверки которых в Societe Generale была создана комиссия. 19 января в ответ на запрос немецкий банк не признал эту транзакцию, после чего трейдер согласился дать признательные показания [49].

Когда удалось выяснить астрономические размеры спекулятивной позиции, генеральный директор и председатель совета директоров Societe Generale Даниэль Бутон заявил о своем намерении закрыть открытую Кервьелем рискованную позицию [49]. На это ушло два дня и привело к убыткам в 4,9 млрд евро.

Возможности инсайдера

Жером Кервьель проработал пять лет в так называемом бэк-офисе банка, т. е. в подразделении, которое непосредственно никаких сделок не заключает. В нем занимаются только учетом, оформлением и регистрацией сделок и ведут контроль за трейдерами. Данная деятельность позволила понять особенности работы систем контроля в банке.

В 2005 г. Кервьеля повысили. Он стал настоящим трейдером. В непосредственные обязанности молодого человека входили элементарные операции по минимизации рисков. Работая на рынке фьючерсных контрактов на европейские биржевые индексы, Жером Кервьель должен был следить за тем, как меняется инвестиционный портфель банка. А его основной задачей, как объяснил один из представителей Societe Generale, было сокращать риски, играя в противоположном направлении: «Грубо говоря, видя, что банк ставит на красное, он должен был ставить на черное». Как у всех младших трейдеров, у Кервьеля был лимит, превышать который он не мог, за этим следили его бывшие коллеги по бэк-офису. В Societe Generale существовало несколько уровней защиты, например трейдеры могли открывать позиции только со своего рабочего компьютера. Все данные об открытии позиций автоматически в реальном времени передавались в бэк-офис. Но, как говорится, лучший браконьер – бывший лесничий. И банк совершил непростительную ошибку, поставив бывшего лесничего в положение охотника. Жерому Кервьелю, имевшему за плечами почти пятилетнюю практику контроля за трейдерами, не составило большого труда обойти эту систему. Он знал чужие пароли, знал, когда в банке проходят проверки, хорошо разбирался в информационных технологиях [50].

Причины

Если Кервьель и занимался мошенничеством, то не в целях личного обогащения. Это говорят его адвокаты, это же признают и представители банка, называя действия Кервьеля иррациональными. Сам Кервьель говорит, что действовал исключительно в интересах банка и хотел только доказать свои таланты трейдера [50].

Последствия

Его деятельность по итогам 2007 г. принесла банку около 2 млрд евро прибыли. Во всяком случае так говорит сам Кервьель, утверждая, что руководство банка наверняка знало, чем он занимается, но предпочитало закрывать глаза до тех пор, пока он был в прибыли [50].

Закрытие открытой Кервьелем рискованной позиции привело к убыткам в 4,9 млрд евро.

В мае 2008 г. Даниэль Бутон покинул пост генерального директора Societe Generale, на этой должности его сменил Фредерик Удеа [51]. Год спустя он был вынужден уйти и с поста председателя совета директоров банка. Причиной ухода стала острая критика со стороны прессы: Бутона обвиняли в том, что подконтрольные ему топ-менеджеры банка поощряли рискованные финансовые операции, осуществляемые сотрудниками банка.

Несмотря на поддержку совета директоров, давление на господина Бутона усиливалось. Его отставки требовали акционеры банка и многие французские политики. Президент Франции Никола Саркози также призвал Даниэля Бутона уйти с поста, после того как стало известно, что в течение полутора лет до скандала компьютерная система внутреннего контроля Societe Generale 75 раз, т. е. всякий раз как Жером Кервьель осуществлял несанкционированные операции, выдавала предупреждение о возможных нарушениях [50].

Сразу после обнаружения потерь Societe Generale создал специальную комиссию по расследованию действий трейдера, в которую вошли независимые члены совета директоров банка и аудиторы PricewaterhouseCoopers. Комиссия пришла к выводу, что система внутреннего контроля в банке была недостаточно эффективной. Это привело к тому, что банк не смог предотвратить столь крупное мошенничество. В отчете говорится, что

«сотрудники банка не проводили систематических проверок» деятельности трейдера, а сам банк не располагает «системой контроля, которая могла бы предотвратить мошенничество» [48].

В отчете о результатах проверки трейдера говорится, что по итогам расследования принято решение «существенно укрепить процедуру внутреннего надзора за деятельностью сотрудников Societe Generale». Это будет сделано при помощи более строгой организации работы различных подразделений банка и координации их взаимодействия. Также будут приняты меры, позволяющие отслеживать и персонифицировать трейдерские операции сотрудников банка посредством «укрепления системы ИТ-безопасности и разработки высокотехнологичных решений по персональной идентификации (биометрии)».

4.2. Формализованное представление угроз ИБ от персонала

4.2.1. Цели моделирования угроз

Моделирование угроз ИБ от персонала является элементом деятельности организации по анализу и оценке соответствующих рисков. С помощью собственной модели угроз ИБ от персонала организация может формализовать имеющиеся у нее знания о таких угрозах, что позволит сформировать эффективную (или по крайней мере адекватную накопленным знаниям) систему защитных мер.

Моделирование угроз ИБ от персонала позволяет ответить на следующие вопросы.

– Кто является источником угрозы?

– Какие причины и условия способствуют реализации угроз ИБ от персонала?

– По какому сценарию может реализоваться угроза?

– К каким последствиям может привести реализация угрозы?

Кроме того, модель угроз ИБ от персонала может быть использована для решения следующих задач в рамках противодействия таким угрозам:

– сопоставление значимости для организации различных угроз ИБ от персонала;

– оценка возможных изменений значимости угроз ИБ от персонала в результате проводимых изменений операционной среды организации;

– поддержка деятельности по разработке в организации внутренних нормативных и организационно-распорядительных документов;

– аналитическое обеспечение деятельности по выявлению областей повышенного риска ИБ от персонала;

– другие задачи, связанные как с принятием решений по защитным мерам, так и с применением защитных мер.

4.2.2. Типология инцидентов

Обобщение мировой практики позволяет выделить следующие типы инцидентов ИБ с участием персонала организации:

– разглашение служебной информации;

– фальсификация отчетности;

– хищение финансовых и материальных активов;

– саботаж деятельности организации;

– злоупотребление служебными полномочиями;

– сокрытие правонарушений.

Под разглашением служебной информации организации (нарушение конфиденциальности служебной информации, утечка) понимается ее распространение за

пределы информационной системы, в которой обрабатывается такая информация, или за пределы круга лиц, которым эта информация доверена.

Можно выделить следующие способы разглашения информации.

– Отчуждение информации, которое состоит в несанкционированном и скрытном копировании небольших фрагментов или значительного массива служебной информации (например, множества документов или базы данных) за пределы области, установленной организацией для хранения этой информации с возможной последующей передачей информационного массива сторонним лицам. Отчуждение может осуществляться внутренним злоумышленником с использованием твердых копий документов (вынос документов, использование почтовой связи) или съемного (флеш-диски и другие портативные накопители) носителя информации, с использованием фото/видеоаппаратуры, а также проводных или беспроводных каналов связи и другими способами.

– Разглашение информации, известной инсайдеру в силу своего служебного положения, третьим лицам, а также предоставление таким лицам консультаций, рекомендаций и аналитических материалов. Такая деятельность может осуществляться в устной форме или путем подготовки инсайдером документа на основе информации, известной инсайдеру в силу своего служебного положения.

Можно выделить следующие способы получения инсайдером разглашаемой служебной информации:

– инсайдер не осуществляет специальный поиск разглашаемой информации, она стала известна ему в результате штатной деятельности из служебных документов и в результате общения с сотрудниками организации; данная информация необходима ему для исполнения служебных обязанностей;

– инсайдер обладает штатным доступом к служебной информации в качестве пользователя информационной системы и может осуществлять поиск необходимых ему материалов в информационной системе по их атрибутам, ознакомление с их содержимым и (или) копирование целиком или отдельными фрагментами;

– инсайдер не обладает штатным доступом к служебной информации, интересующей сторонних лиц, и запрашивает соответствующие дополнительные полномочия, мотивируя некоторой правдоподобной служебной необходимостью;

– инсайдер осуществляет несанкционированное получение информации, используя слабости системы разграничения доступа, осуществляя кражу носителей или оборудования, восстановление остаточной информации, используя специальную аппаратуру или программные средства для съема или перехвата информации, используя приемы социальной инженерии, идентификатор и прочие атрибуты безопасности другого пользователя, ошибки персонала и другие возможности;

– инсайдер выполняет обязанности администратора в информационной системе, а информация, обрабатываемая в данной системе, оказывается доступна ему для ознакомления или копирования как лицу с полномочиями системного администратора;

– инсайдер получает служебную информацию при устном неформальном общении с другими инсайдерами, обладающими такой информацией;

– инсайдер получает информацию путем анализа и обобщения фактов, фрагментов информации, полученных им из различных источников – штатным образом, путем наблюдения за поведением и общением субъектов, за распорядком деятельности и т. д.;

– инсайдер получает служебную информацию в результате сговора с другим инсайдером, получившим доступ к информации одним из перечисленных в настоящем перечне способов.

Разглашенная инсайдером служебная информация может быть объединением фрагментов информации, полученной различными способами из числа приведенных выше.

Фальсификация отчетности состоит в умышленном представлении ложных или

искаженных отчетов по результатам некоторой деятельности. Собственно фальсифицируемые отчеты, могут относиться как к внутренней деятельности организации, так и к отношениям организации с внешними структурами (государственными органами, материнской компанией, дочерними компаниями, кредиторами).

По целям фальсификация отчетности может быть классифицирована следующим образом:

– сокрытие или, напротив, демонстрация неудовлетворительных показателей деятельности;

– демонстрация завышенных результатов деятельности для получение поощрения или дополнительного трудового вознаграждения;

– введение в заблуждение контрагентов организации;

– введение в заблуждение регулирующих и правоохранительных органов;

– сокрытие нарушений законов, требований регулирующих органов, внутренних нормативных актов организации.

Хищение (финансовых или материальных) активов – это совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение активов (принадлежащих организации, ее контрагентам, третьим лицам) в пользу злоумышленника или других лиц, причинившие ущерб лицам, обладающим правами в отношении данных активов (например, собственнику, арендатору, залогодержателю).

Хищение финансовых и материальных активов включает следующие категории преступлений:

– кража;

– присвоение и растрата активов;

– различные формы мошенничества, связанного с осуществлением основной, вспомогательной и управленческой деятельности в организации.

Наиболее распространены следующие формы мошенничества:

– мошенничество, связанное с отношениями с поставщиками;

– мошенничество, связанное с отношениями с клиентами;

– кредитное и инвестиционное мошенничество;

– вексельное мошенничество;

– мошенничество при использовании банковских гарантий и поручительств;

– мошенничество со счетами;

– вброс подложных или модификация корректных платежных документов;

– мошенничество с пластиковыми картами (фальшивые карты и операции);

– депозитное мошенничество;

– мошенничество, связанное с внутренней хозяйственной деятельностью организации, в частности, обязательствам по трудовым соглашениям.

Саботаж – это умышленное создание препятствий для осуществления некоторой деятельности организации, что уменьшает возможность реализации целей организации.

По целями саботажа инциденты могут быть классифицированы следующим образом:

– снижение репутации организации, например, компрометация качества определенных услуг, предоставляемых организацией, или иное нанесение ущерба отношениям организации с клиентами, например, с целью завладения клиентской базой организации;

– саботаж деятельности контрагентов организации;

– срыв, создание помех, манипулирование и оказание иных воздействий на управление, осуществление и результат некоторой бизнес-деятельности, вспомогательной деятельности или отдельного проекта организации, например, для получения конкурентами организации и иными субъектами рыночных отношений определенных преимуществ, создания условий, препятствующих обеспечению организацией своих законных прав;

– саботаж мер безопасности, используемых организацией, и создание уязвимостей с целью снижения защищенности информационных активов организации перед внешними и внутренними угрозами;

– сокрытие следов, создание ложных следов, ложных версий и иных помех для расследования некоторой противоправной деятельности;

– манипулирование рынками ценных бумаг путем создания «негатива» в связи с информацией о происшествии в организации;

– месть в отношении организации или отдельных сотрудников организации;

– экстремистские, террористические, политические и подобные цели.

Сокрытие правонарушения – это создание препятствий обнаружению и регистрации правонарушения.

Сокрытие правонарушений, в том числе различных видов корпоративных правонарушений может осуществляться в форме саботажа, фальсификации отчетности, а также в виде самостоятельного нарушения с использованием модификации, удаления, вброса информации или несанкционированной модификации программных и аппаратных средств.

Злоупотребление полномочиями – это использование инсайдером своих полномочий в целях извлечения не разрешенных организацией выгод и преимуществ для себя, что осуществляется путем выполнения или невыполнения каких-либо действий, связанных со служебными обязанностями инсайдера. К злоупотреблению полномочиями не относятся правонарушения, которые квалифицируются как хищение или саботаж.

В частности, к злоупотреблениям полномочиями относят:

– манипуляции, связанные с услугами, предоставляемыми организацией, например, создание необоснованных преимуществ или помех для определенных клиентов;

– манипуляции, связанные с закупками, осуществляемыми организацией, например создание необоснованных преимуществ для определенных поставщиков;

– манипуляция действиями организации в иных сферах ее деятельности (на различных рынках, в стратегическом планировании, в инвестиционных проектах, в сфере внутренней хозяйственной деятельности, в сфере и др.).

4.2.3. Факторная модель

Риски ИБ от персонала составляют отдельную группу рисков ИБ организации, однако спектр причин и условий их реализации очень широк. Мы предлагаем описывать риски ИБ от персонала в виде факторной модели – системы причин и условий, благоприятствующих реализации таких рисков. Общая структура факторной модели рисков ИБ от персонала представлена на рис. 63.

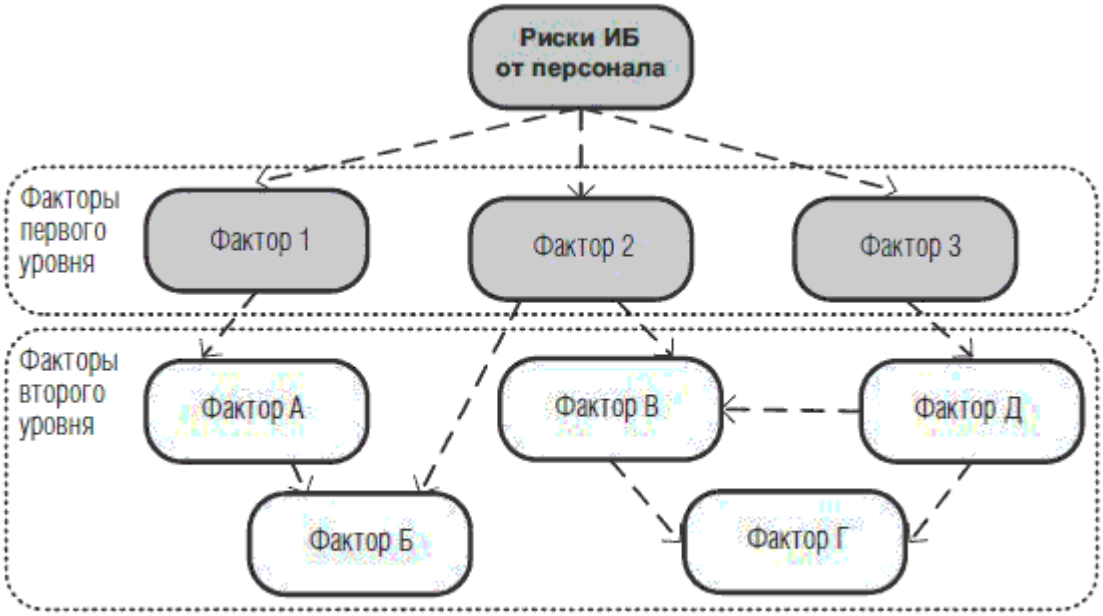


Рис. 63. Общая структура факторной модели рисков ИБ от персонала

Факторы риска связаны в единую сеть причинно-следственными связями. Конечным (и наиболее значимым для организации) узлом причинно-следственной сети является узел «Риски ИБ от персонала».

В факторной модели факторы риска разделены на два уровня:

– факторы риска второго уровня – сравнительно мелкие явления, которые могут отрабатываться (оцениваться, управляться) организацией по отдельности, между факторами этой группы существуют многочисленные связи, возможны циклы как положительной, так и отрицательной обратной связи;

– факторы риска первого уровня непосредственно влияют на реализацию рисков, они консолидируют влияние всего множества факторов риска второго уровня и позволяют упростить работу с моделью.

Факторы риска второго уровня необходимы в модели из-за многочисленности и сетевой структуры факторов первого уровня. Связи внутри группы факторов второго уровня отсутствуют.

Факторы риска первого уровня – это явления, которые непосредственно и наиболее сильно влияют на возможность реализации угроз ИБ от персонала в организации. Вариант системы факторов риска первого уровня приведен в таблице 11. Для факторов приведены краткие описания.

Перечисленные факторы риска первого уровня могут быть отображены (детализированы) в систему факторов риска второго уровня – более мелких (и поэтому более понятных) явлений, способствующих реализации угроз ИБ от персонала. Подготовленный нами вариант такого отображения представлен в таблице 12 и совершенно определенно не исчерпывает многогранной природы угроз ИБ от персонала. Отметим, что некоторые факторы второго уровня повторяются для нескольких факторов первого уровня, поскольку влияют на них одновременно.

Таблица 11

Факторы риска первого уровня

Фактор риска первого уровня	Природа фактора риска	Негативное воздействие фактора риска
1. Наличие у сотрудника организации мотивов для нападения	Возможность возникновения у инсайдера конфликта личных и служебных интересов	Внутренний злоумышленник пренебрегает интересами организации, осуществляя целенаправленные действия по подготовке и проведению нападения
2. Концентрация полномочий у одного сотрудника	Естественная неопределенность, характерная для задачи управления полномочиями. Стремление ответственных лиц организации «уменьшить издержки», возникающие при применении механизмов разделения полномочий	Внутренний злоумышленник при реализации своей цели злоупотребляет полномочиями, не сталкиваясь с какими-либо ограничениями
3. Наличие у многих сотрудников эксклюзивных знаний в отношении бизнеса организации и (или) операционной среды	Наличие сотрудников с большим и разнообразным опытом работы, что следует из потребности организации в увеличении числа квалифицированных и опытных сотрудников. Слабости, связанные с распространением знаний внутри организации, — естественные и привнесенные ограничения на распространение знаний. Естественная склонность организации к эмпирическому знанию в противовес формально закрепленному, «книжному» знанию. Естественная склонность сотрудников к сокрытию знаний. Признание в организации «высоким» статуса лица с «сильными» скрытыми знаниями. Коллизия обратной связи: организация стремится к распространению знаний, однако опасается эксклюзивных знаний сотрудников	Внутренний злоумышленник использует знание операционной среды организации для построения эффективной схемы атаки
4. Сложность контроля деятельности сотрудников и выявления нарушений	Естественная неопределенность, характерная для деятельности сотрудников. Стремление ответственных лиц организации «уменьшить издержки», возникающие при применении мер контроля	Нападение со стороны внутреннего злоумышленника сложно выявить, сложно определить виновного и прилечь его к ответственности

Продолжение табл. 11

Фактор риска первого уровня	Природа фактора риска	Негативное воздействие фактора риска
5. Слабая регламентация различных видов деятельности, осуществляемых в организации	Организация ориентируется на профессионализм сотрудников, значительную свободу их действий и высокий уровень доверия к сотрудникам. Данный подход представляет противоположность «механистичной» ориентации на четко расписанные регламенты «на все случаи жизни»	Действия инсайдера в среде без установленных формальных правил не могут быть интерпретированы как допустимые или недопустимые (соответствующие или не соответствующие интересам организации) без тщательного анализа контекста и содержания таких действий
6. Не мотивированные с точки зрения бизнеса изменения операционной среды организации	В организации осуществляются естественные процессы самоулучшения в некоторой области вспомогательной деятельности. Такие процессы опасны, если их цели не связаны прямо с основной деятельностью, а связаны с совершенствованием вспомогательной деятельности	Информационные активы организации в течение значительных интервалов времени находятся в уязвимом состоянии. Нарушается адекватность операционной среды организации требованиям бизнеса
7. Слабая детерминированность процессов основной деятельности организации. Возникновение необходимости реализации деятельности в организации за пределами регламентов, поскольку организация вынуждена искать различные способы реализовать цель в условиях изменчивой среды	Изменчивость бизнес-среды. Объективная невозможность заранее описать необходимые действия во всех возникающих ситуациях	Действия инсайдера в обстановке без установленных формальных правил не могут быть интерпретированы как допустимые или недопустимые (соответствующие или не соответствующие интересам организации) без тщательного анализа контекста и содержания таких действий
8. Неадекватность установленных отношений владения информационными активами	Естественная неопределенность владения активами. «Разрывы», недостатки, возникающие в результате смены владения активами	Внутренний злоумышленник пользуется неопределенным статусом, «бесхозностью» информационного актива

Окончание табл. 11

Фактор риска первого уровня	Природа фактора риска	Негативное воздействие фактора риска
9. Сговор внешнего и внутреннего злоумышленников	Объективная невозможность реализации внутренним злоумышленником некоторых форм нападения без внешней поддержки	Деятельность внутреннего злоумышленника активно поддерживается извне, а результат атаки конвертируется в выгоду для него через взаимодействие с внешним сообщником
10. Кадровые проблемы (недостаточная лояльность и благонадежность персонала)	Морально-нравственное состояние современного общества. Характер действующего законодательства, которое путем предоставляет значительные права работникам и за счет этого ограничивает возможности работодателя по защите своих интересов	Низкий уровень сопротивления личности инсайдера в отношении соблазнов использования служебных полномочий
11. Объективная неадекватность функциональности информационных систем организации требованиям бизнеса, в частности, избыточность функциональности информационных систем	Невозможность детально определить требования к информационной системе на этапе проектирования. Необходимость обеспечить совместимость информационной системы с открытыми стандартами. Зависимость организации от готовых, «коробочных» продуктов. Создание информационной системы «на перспективу» с учетом возможных функциональных потребностей за счет избыточного функционала	Использование избыточной функциональности внутренним злоумышленником для организации атаки, например, создание скрытого канала для отчуждения информации
12. Злоупотребление доверием других сотрудников организации	Объективная потребность в отношениях доверия между сотрудниками организации для реализации целей деятельности организации	Использование внутренним злоумышленником для реализации своей цели полномочий и знаний других сотрудников организации
13. Неопределенность в отношении адекватности принимаемого организацией риска, связанного с угрозами ИБ от персонала	Неопределенность, характерная для любого прогноза. Неспособность организации оценивать и управлять значительным числом факторов риска ИБ от персонала	Неспособность принятых организацией защитных мер результативно противодействовать той угрозе, для которой они предназначены

Таблица 12

Двухуровневая система факторов риска ИБ от персонала

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
1. Наличие у сотрудника организации мотивов для нападения	Наличие сильных неформальных структур в организации	Неформальные отношения развиты в организации настолько, что оказывают существенное влияние на формальные, установленные в рамках организационной структуры и бизнес-процессов, что порождает конфликт интересов
	Осведомленность сотрудников организации о спросе на служебную информацию организации со стороны внешних организаций	Возможно возникновение материальной заинтересованности в передаче служебной информации третьим лицам
	Неблагоприятный моральный психологический климат в коллективе организации	Возможен конфликт интересов на почве личной неприязни сотрудников. Отсутствие доверия между сотрудниками ухудшает информационные процессы. Возможно возникновение враждующих кланов внутри организации
	Неудовлетворенность персонала организации условиями труда, в частности, уровнем оплаты труда	Вероятно возникновение заинтересованности в дополнительном заработке, намерений смены работы
	«Близость» значительной части персонала к операциям над материальными активами, которые осуществляются в организации как ИТ-процессы	Возможно возникновение у сотрудника соблазна воздействия на операции в корыстных целях. Сотрудник представляет интерес для внешних злоумышленников
	Наличие у сотрудников индивидуальных особенностей, проблем и мотивов, способных при неблагоприятных условиях подтолкнуть сотрудника к действиям против интересов организации	—
	Невозможность адекватно наказать выявленного нарушителя	Отсутствие опасных последствий создает у потенциального нарушителя уверенность в безнаказанности и снижает порог принятие решения о нападении
	Возможность приема на работу в организацию недостаточно благонадежных лиц	—

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Оказание давления на сотрудника организации внешними злоумышленниками тем или иным способом (угрозы близким сотрудника, угрозы в отношении имущественных или других прав сотрудника)	Внешнее принуждение делает возможным нападение даже со стороны самого благонадежного сотрудника
	Накопление у сотрудника критической массы существенных и незначительных негативных мотивов	Даже незначительные мотивы (как связанные с работой в организации, так и не связанные) в совокупности способны реализоваться в нападении, особенно если сотрудник оказался в тяжелых психологических условиях
2. Концентрация полномочий у одного сотрудника	Возможность действий потенциального внутреннего злоумышленника, направленных на расширение служебных полномочий	Любое расширение полномочий увеличивает область легальных действий и снижает возможности организации по контролю. Запрос на расширение полномочий почти всегда мотивирован благовидным предлогом
	Недостатки осуществляемой организацией деятельности по управлению информационными активами	Опасность представляют следующие обстоятельства: — наличие неучтенных (ничьих) активов; — появление и хождение активов различной формы, но одного содержания; — сложность определения происхождения, истории и уровня ценности для организации произвольно взятого актива в ее информационной системе; — сложность управления распространением активов; — отсутствие разделения ролей при доступе к активам; — слабости в процедурах утилизацией информационных активов; — ситуации концентрации активов; — отсутствие контроля за фактически предоставленными правами использования активов

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Наличие избыточных служебных полномочий, предоставленных сотруднику	Избыточные полномочия создают расширенную область легальных действий и снижают возможности организации по контролю. Концентрация полномочий может возникнуть в силу различных причин: недостатка персонала, из-за замещения при временном отсутствии сотрудника, в силу сложившихся в коллективе личных отношений
	Значительные возможности администраторов систем по управлению конфигурацией и правами доступа, а также по доступу к обрабатываемой информации	Административный доступ к компонентам информационной системы обычно является доступом без технических ограничений. Даже если политика ИБ организации накладывает определенные ограничения, такие ограничения почти никогда не поддерживаются соответствующими аппаратными или программными средствами
	Возможность преодоления защитных мер, ограничивающих полномочия сотрудников	В отличие от внешнего злоумышленника инсайдер имеет более высокие шансы на преодоление защитных мер, поскольку обладает необходимым временем, базовыми полномочиями доступа (физическим, сетевым), знаниями, а также пользуется доверием со стороны организации
	Возможность нецелевого использования служебных полномочий (злоупотребления полномочиями)	Все возможные ситуации применения полномочий сотрудника регламентировать невозможно. Осуществлять тотальный контроль целевого применения полномочий также трудоемко и накладно для организации. Это обусловливает риски злоупотребления полномочиями
	Недостаточные возможности защитных мер ограничения полномочий	Установленные политики ИБ в части ограничения полномочий не поддержаны в достаточной мере соответствующими техническими, программными и организационными мерами. Выполнение ограничений внутренним злоумышленником под вопросом

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Сложность разграничения физического доступа	Любой сотрудник на практике обладает гораздо более широким доступом в помещения и к объектам ИТ-инфраструктуры, чем это необходимо организации
	Возможность завладения полномочиями других сотрудников, Возможность действия с их полномочиями и под их идентификатором	Наиболее привлекательным объектом для нападения, вероятно, являются атрибуты безопасности сотрудника, обладающего наибольшими полномочиями. Замаскированный таким образом злоумышленник не без оснований чувствует себя защищенным и весьма опасен
	Возможность установки нештатных программных и аппаратных средств доступа к информационным активам	Естественным способом расширения возможностей инсайдера является расширение функциональных возможностей информационной системы. Собственно установка нештатных программных и аппаратных средств в случае выявления может быть мотивирована служебной необходимостью
	Возможность использования внутренним злоумышленником неопределенностей, возникающих в нештатных и аварийных ситуациях	Нештатные и аварийные ситуации могут быть удобным прикрытием для нападения или сокрытия его следов. Точный сценарий действий в любой нештатной ситуации заранее регламентировать невозможно, при том что обычно предъявляются требования по скорейшему устранению нештатной ситуации. В нештатной ситуации создаются легальные возможности бесконтрольной деятельности как в рамках, так и за пределами полномочий
	Недостаточное осознание проблем ИБ руководителями структурных подразделений организации	Руководитель подразделения задает тон отношения сотрудников к проблемам ИБ, которое, в свою очередь, определяет качество применяемых в подразделении защитных мер
	Существование видов деятельности сотрудников, результат которых невозможно предсказать	Естественная неопределенность относительно положительного результата деятельности сотрудника создает сложности ее контроля, поскольку неясно, как результат соотносился с действиями сотрудника

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом
	Сложность штатной деятельности сотрудника	Сложность штатной деятельности сотрудника позволяет ему обосновать избыточные полномочия и снижает возможности контроля такой деятельности
	Действия организованной группы внутренних злоумышленников	Организованная группа имеет значительно больше возможностей реализовать цель в рамках штатных полномочий, чем злоумышленник-одиночка. Во-первых, полномочия и знания группы больше. Во-вторых, действия нескольких лиц гораздо труднее ассоциировать при мониторинге и расследовании. Таким образом, может быть достигнута более высокая скрытность. Группа злоумышленников может реализовать цель более высокого уровня, чем одиночка
3. Наличие у многих сотрудников эксклюзивных знаний в отношении бизнеса организации и (или) ее операционной среды	Возможность сокрытия (несообщения) инсайдером информации об обнаруженной уязвимости	Сотрудник организации имеет наибольшие возможности выявления уязвимостей системы защиты организации. Известные некоторому кругу лиц, но неизвестные организации уязвимости могут обуславливать серьезные риски
	Возможность изучения внутренним злоумышленником системы защиты с целью выявления границ ее возможностей	В отличие от внешнего злоумышленника инсайдер обладает легальными возможностями получать знания, необходимые для обхода системы защиты

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Возможность поиска «бесхозных» информационных активов и проверки возможностей их бесконтрольного и безнаказанного использования	В отличие от внешнего злоумышленника инсайдер обладает легальными возможностями выявления ценных целей из числа уязвимых, а также активной проверки системы защиты этих целей
	Наличие у разработчиков значительных знаний об уязвимостях компонентов информационной системы	Разработчик информационной системы, принимающий непосредственное участие в ее промышленной эксплуатации, — признанный в международной практике риск
	Возможность изучения инсайдером технической документации информационной системы и исходных кодов программных средств	Подробно документированный программный компонент, а тем более доступный организации в исходных кодах не только большой плюс для его эксплуатации и сопровождения, но и риск того, что внутренний злоумышленник обнаружит уязвимость
	Значительные знания инсайдеров о тонких особенностях системы защиты, определяющих ее предсказуемость, и возможностях преодоления системы защиты	К особенностям системы защиты можно отнести уязвимости технических средств, проблемы системы регистрации действий и других событий, временная неработоспособность или перегруженность службы ИБ, время и задачи предстоящей проверки, слабо контролируемые организацией области деятельности сотрудников
	Прогнозирование инсайдером возникновения нештатной или аварийной ситуации	Внутренний злоумышленник, даже не инсценируя аварию, может предсказать ее возникновение, подготовиться и воспользоваться результатом
	Возможность исследования информационной системы и технологических процессов организации внутренним злоумышленником с целью выявления целей для нападения и уязвимостей	Исследование внутренним злоумышленником информационной системы и технологических процессов организации может осуществляться как в активном (инсценировка ситуаций, наблюдение и анализ реакции), так и в пассивном (наблюдение и анализ) режиме
	Осведомленность инсайдеров о спросе на служебную информацию организации со стороны внешних организаций	Такая осведомленность может возникнуть как в результате контакта с внешними заинтересованными организациями, так и в результате анализа инсайдером конкурентной среды организации

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Бывшие сотрудники, обладающие значительными знаниями	Уход сотрудника — зачастую это утечка (а порой и безвозвратная потеря) важной информации об особенностях операционной среды организации. Усугубляет ситуацию возможность его трудоустройства в конкурирующую организацию
	Несоответствие регламентов деятельности реальной операционной среде и процессам организации	Если сотрудник не может действовать по регламенту, он будет действовать, как считает необходимым. В этом случае становятся неэффективными многие защитные меры, а расследование инцидентов не позволит выявить виновника
	Кадровые изменения	Изменения состава сотрудников, реализующих некоторую деятельность, может повлиять как на качество результатов этой деятельности, так и на ее защищенность от угроз. Существенный риск связан с процессом «вхождения» каждого нового сотрудника в роль (должность), с получением сотрудником необходимых знаний, с неизбежными ошибками и т. д.
	Действия организованной группы внутренних злоумышленников	Организованная группа имеет значительно больше возможностей реализовать цель в рамках штатных полномочий, чем злоумышленник-одиночка. Во-первых, полномочия и знания группы больше. Во-вторых, действия нескольких лиц гораздо труднее ассоциировать при мониторинге и расследовании. Таким образом, может быть достигнута более высокая скрытность. Группа злоумышленников может реализовать цель более высокого уровня, чем одиночка
4. Сложность контроля деятельности сотрудников и выявления нарушений	Возможности разработчиков и администраторов по внесению изменений в функциональность и конфигурацию информационных систем организации	Сложность информационных систем обычно не позволяет организации своевременно и в полном объеме контролировать вносимые в них (ввиду той или иной необходимости) изменения с точки зрения последствий для защищенности этих систем

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Недостатки осуществляемой организацией деятельности по управлению информационными активами	Опасность представляют следующие обстоятельства: — наличие неучтенных (ничьих) активов; — появление и хождение активов различной формы, но одного содержания; — сложность определения происхождения, истории и уровня ценности для организации произвольно взятого актива в ее информационной системе; — сложность управления распространением активов; — отсутствие разделения ролей при доступе к активам; — слабости в процедурах утилизацией информационных активов; — ситуации концентрации активов; — отсутствие контроля за фактически предоставленными правами использования активов
	Наличие избыточных служебных полномочий, предоставленных сотруднику	Избыточные полномочия создают расширенную область легальных действий и снижают возможности организации по контролю. Концентрация полномочий может возникнуть в силу различных причин: недостатка персонала, из-за замещения при временном отсутствии сотрудника, в силу сложившихся в коллективе личных отношений
	Недостатки процедур расследования инцидентов ИБ	Недостатки не позволяют выявить предпосылки инцидента и построить его ретроспективную картину. Это существенно влияет на возможность обнаружения виновных лиц, на возможность выявления проблем, способствовавших инциденту, а также на возможность накопления знаний службой ИБ организации

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Нарушение функциональности средств защиты	Применяемые организацией защитные меры в силу различных причин могут бездействовать в течение некоторого периода рабочего времени — «окна» уязвимости. При этом риски соответственно повышаются
	Существование ролей (или должностей), объективно требующих значительных полномочий	Даже если в организации проведена серьезная работа по оптимизации системы ролей, некоторым ролям (должностям) все равно будут назначены значительные (по сравнению с другими) полномочия. Соответственно, связанные с их исполнителями риски значительно выше, чем риски от других сотрудников
	Возможность противодействия расследованию инцидентов со стороны внутреннего злоумышленника	Не выявленный организацией (а иногда и выявленный) внутренний злоумышленник, вероятно, будет препятствовать расследованию инцидента, используя служебные полномочия и доверие организации: скрывать следы нападения, создавать ложные версии, дискредитировать работу ведущей внутреннее расследование группы
	Риск неустановления причин и обстоятельств инцидента ИБ	Часто крайне сложно установить и документально подтвердить точный характер инцидента, наличие среди причин умышленных действий и тем более личность виновного лица. Такие слабости закономерно сформируют ощущение безнаказанности у внутреннего злоумышленника
	Возможность для сокрытия инсайдерами реальной цели их действий в информационной системе организации	Двусмысленность, непрозрачность многих операций в информационной системе связана с объективной сложностью как ИТ, так и деятельности организации
	Отсутствие канала связи (горячей линии) между сотрудниками организации и службой ИБ организации	Недостаточная осведомленность службы ИБ о нештатных ситуациях, связанных с работой информационной системы

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Возможность завладения полномочиями других сотрудников. Возможность действия с их полномочиями и под их идентификатором	Наиболее привлекательным объектом для нападения, вероятно, являются атрибуты безопасности сотрудника, обладающего наивысшими полномочиями. Замаскированный таким образом злоумышленник не без оснований чувствует себя защищенным и весьма опасен
	Возможность установки нештатных программных и аппаратных средств доступа к информационным активам	Естественным способом расширения возможностей инсайдера является расширение функциональных возможностей информационной системы. Собственно, установка нештатных программных и аппаратных средств в случае выявления может быть мотивирована служебной необходимостью
	Возможность использования внутренним злоумышленником неопределенностей, возникающих в нештатных и аварийных ситуациях	Нештатные и аварийные ситуации могут быть удобным прикрытием для нападения или сокрытия его следов. Точный сценарий действий в любой нештатной ситуации заранее регламентировать невозможно, при том что обычно предъявляются требования по скорейшему устранению нештатной ситуации. В нештатной ситуации создаются легальные возможности бесконтрольной деятельности как в рамках, так и за пределами полномочий
	Недостаточный контроль за соблюдением нормативно-распорядительных документов организации	Наличие норм не означает автоматического их выполнения персоналом. Без системы контрольных мер масса незлоумышленных ненаказанных нарушений скроет под плотной завесой действия внутреннего злоумышленника
	Невозможность ассоциировать события, наблюдаемые службой ИБ и подразделениями, ответственными за другие области безопасности (кадровую, физическую, экономическую)	Организационные границы подразделений безопасности организации и несовместимость используемых ими технологий и форм представления информации не позволяют обмениваться информацией, которая в совокупности может быть полезной для выявления возможных злоумышленников

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Регистрационная информация не хранится в течение достаточно продолжительного интервала времени	Довольно сложно поддерживать единую политику хранения регистрационной информации с различных объектов. Это может привести к отсутствию необходимой для контроля или расследования информации
	Привязанность регистрационной информации к контексту деятельности	На момент анализа регистрационной информации контекст анализируемой ситуации (состав используемых объектов — файлы и таблицы, вычислительные процессы, пользователи и пр.) может значительно измениться, из-за чего не только сложно дать оценку рассматриваемой ситуации, но и понять, что вообще происходило. Контекстная информация почти никогда не собирается в достаточном для результативного анализа журналов регистрации объеме
	Возможность активного противодействия злоумышленника эффективной регистрации событий	Среди вариантов активного противодействия — воздействие на выбор параметров регистрации событий (исключение существенных событий или атрибутов событий), переполнение или удаление журнала регистрации
	Неоднородность системных и прикладных платформ, используемых организацией	Технический и программный «зоопарк» создает многочисленные сложности как в управлении ИТ, так и в управлении ИБ организации
	Уязвимость информационной системы в период внесения изменений	Период внесения изменений — всегда окно уязвимости, когда производятся критичные и слабо контролируемые операции в промышленной системе
	Слабая защищенность журналов регистрации компонентов информационных систем	В большинстве технических и программных компонентов информационных систем журналы регистрации устроены собственным, уникальным способом. Защищенность многих журналов оставляет желать лучшего, что создает для внутреннего злоумышленника возможности сокрытия следов

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Толерантность к нарушениям различного рода в коллективе организации	Атмосфера терпимости к наблюдаемым в коллективе нарушениям способствует сокрытию настоящих нападений, бессилию службы ИБ, исчезновению факторов, сдерживающих действия инсайдеров против интересов организации
	Несоответствие регламентов деятельности реальной операционной среде и процессам организации	Если сотрудник не может действовать по регламенту, он будет действовать, как считает необходимым. В этом случае становятся неэффективны многие защитные меры, а расследование инцидентов не позволит выявить виновника
	Значительный поток тревожных событий от системы мониторинга ИБ, затрудняющий их обработку	Сложность представляет анализ потока событий ИБ от всей информационной системы организации, поскольку такой анализ фактически требует моделирования работы информационной системы
	Отсутствие мер мониторинга конфигурации информационной системы	—
	Неспособность средств ограничения полномочий регистрировать в достаточном объеме информацию о фактах использования полномочий	Некоторые средства ограничения полномочий не могут эффективно действовать в качестве «контрольных точек». Эффект от применения «барьерных» средств защиты (средств разграничения доступа, антивирусов, межсетевых экранов) значительно повышается, если они ведут журнал регистрации
	Возможность уничтожить, подменить или иным образом скрыть следы злоумышленной деятельности	Можно быть уверенным, что внутренний злоумышленник постарается снизить вероятность обнаружения всеми доступными ему средствами
	Сложность регистрации событий физического доступа	Регистрация физического доступа в помещения и к объектам ИТ-инфраструктуры все еще является дорогостоящей и сильно уязвимой защитной мерой

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Неспособность прикладных компонентов информационной системы действовать в качестве источников информации о доступе и деятельности пользователей (контрольных точек)	Потенциально любому приложению доступна семантика действий пользователей на уровне прикладных операций. Однако крайне мало приложений, которые ведут собственный качественный журнал регистрации таких действий
	Сложность обнаружения аномалий в ходе технологических процессов и сложность анализа и оценки таких аномалий	—
	Возникновение ошибок обнаружения первого и второго рода в системах выявления нарушений	Ложные тревоги системы мониторинга вынуждают службу ИБ (и другие подразделения) тратить ресурсы на понимание вызвавших ложную тревогу ситуаций. Такие ошибки вместе с ошибками необнаружения нападения являются характерной особенностью всех существующих систем мониторинга. Постоянные ошибки подрывают доверие к средствам мониторинга и снижают бдительность службы ИБ
	Сложность своевременного обнаружения признаков подготовки или проведения атаки	Внутренний злоумышленник действует скрытно, используя при маскировке знания о применяемых организацией мерах контроля
	Деградация функций системы мониторинга со временем	Состав собираемых событий и модель их анализа обычно отстают от развития контролируемой информационной системы, что является причиной снижения эффективности системы мониторинга
	Возможность осуществления внутренним злоумышленником распределенной атаки	Целью распределенной атаки может быть отвлечение внимания службы ИБ на ложные цели и следы, сокрытие истинной цели нападения
	Наличие недостатков в системе мониторинга ИБ	Различные недостатки систем мониторинга ИБ снижают возможности контроля действия пользователей в пределах их полномочий

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Отсутствие инцидентов безопасности и снижение бдительности сотрудников службы ИБ	—
	Недостаточная бдительность сотрудников организации	—
	Сложность регистрации событий физического доступа	Регистрация физического доступа в помещения и к объектам ИТ-инфраструктуры все еще является дорогостоящей и сильно уязвимой защитной мерой
	Существование видов деятельности сотрудников, результат которых невозможно предсказать	Естественная неопределенность относительно положительного результата деятельности сотрудника создает сложности ее контроля, поскольку не ясно, как результат соотносился с действиями сотрудника
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом
	Сложность штатной деятельности сотрудника	Сложность штатной деятельности сотрудника позволяет ему обосновать избыточные полномочия и снижает возможности контроля такой деятельности
	Наличие и эффективность мер по обеспечению учетности фактов использования сотрудниками служебных полномочий	Регистрация фактов использования полномочий позволяет как минимум обеспечить в информационном отношении внутренние расследования

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
5. Слабая регламентация различных видов деятельности, осуществляемых в организации	Недостатки осуществляемой организацией деятельности по управлению информационными активами	Опасность представляют следующие обстоятельства: — наличие неучтенных (ничьих) активов; — появление и хождение активов различной формы, но одного содержания; — сложность определения происхождения, истории и уровня ценности для организации произвольно взятого актива в ее информационной системе; — сложность управления распространением активов; — отсутствие разделения ролей при доступе к активам; — слабости в процедурах утилизацией информационных активов; — ситуации концентрации активов; — отсутствие контроля за фактически предоставленными правами использования активов
	Возможность использования внутренним злоумышленником полномочий и знаний других сотрудников в рамках служебных или неформальных отношений	Подобная ситуация — один из побочных эффектов атмосферы доверия к организации. Зачастую проще всего обмануть самых лучших и старательных сотрудников, поскольку они часто сконцентрированы на своей основной задаче и могут упустить из внимания факты, не относящиеся к такой задаче
	Нарушение согласованности управления доступом к совместно используемым ресурсам в случае, когда владельцы и пользователи активов относятся к различным организационным подразделениям	Когда обмен информацией и потребностями затруднен в результате различной организационной подчиненности сотрудников, назначенные права доступа, как правило, избыточны по сравнению с необходимыми
	Неоднозначность и противоречивость системы нормативно-распорядительных документов организации	Неопределенность, порождаемая слабостями нормативной базы, приводит к массовым нарушениям установленных норм, неопределенному правовому статусу действий сотрудников, невозможности реализации политики ИБ, резкому росту возможностей злоумышленной деятельности

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Недостаточно детальная регламентация процессов деятельности организации	Слабая регламентация создает неопределенности как в части объема полномочий субъектов, так и в части ситуаций их применения, что затрудняет применение других защитных мер почти всех видов
	Проблемы в управлении организацией в целом или ее структурными подразделениями	В качестве примеров проблем можно привести несоответствие циклов улучшения организации темпу изменениям среды, неадекватное распределение ресурсов и т. п.
	Возможность конфликта интересов между подразделениями организации при осуществлении некоторых процессов ИБ (мониторинг, расследование инцидентов ИБ и др.)	Реализация защитных мер, на которых настаивает служба ИБ может оказаться нежелательной с точки зрения службы ИТ, а применение защитных мер может показаться неудобным пользователям
	Несоответствие регламентов деятельности реальной операционной среде и процессам организации	Если сотрудник не может действовать по регламенту, он будет действовать, как считает необходимым. В этом случае становятся неэффективны многие защитные меры, а расследование инцидентов не позволит выявить виновника
	Существование видов деятельности сотрудников, результат которых невозможно предсказать	Естественная неопределенность относительно положительного результата деятельности сотрудника создает сложности ее контроля, поскольку не ясно, как результат соотносился с действиями сотрудника
	Сложность штатной деятельности сотрудника	Сложность штатной деятельности сотрудника позволяет ему обосновать избыточные полномочия и снижает возможности контроля такой деятельности
6. Не мотивированные с точки зрения бизнеса изменения операционной среды организации	Возможности разработчиков и администраторов по внесению изменений в функциональность и конфигурацию информационных систем организации	Сложность информационных систем обычно не позволяет организации своевременно и в полном объеме контролировать вносимые в них (ввиду той или иной необходимости) изменения с точки зрения последствий для защищенности этих систем

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Недостаточная компетентность персонала	Отсутствие опыта, знаний или стремления к достижению качественного результата деятельности порождает массу скрытых и явных проблем, способствующих реализации преднамеренных угроз ИБ от персонала
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом
	Проблемы в управлении организацией в целом или ее структурными подразделениями	В качестве примеров проблем можно привести несоответствие циклов улучшения организации темпу изменениям среды, неадекватное распределение ресурсов и т. п.
	Естественная изменчивость ИТ-среды организации	Внешняя по отношению к организации среда динамична. Организация реагирует изменением внутренней среды, в том числе бизнес-процессов, структуры, ИТ-среды. Защитные меры почти всегда отстают от изменений внутренней среды, что создает определенную уязвимость
	Уязвимость информационной системы в период внесения изменений	Период внесения изменений — всегда окно уязвимости, когда производятся критичные и слабо контролируемые операции в промышленной системе
	Отсутствие мер мониторинга конфигурации информационной системы	—
	Халатность сотрудников организации	Способствует реализации преднамеренных угроз. Наряду с ошибкой может использоваться злоумышленником в качестве прикрытия преднамеренных действий

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Недостаточное осознание проблем ИБ руководителями структурных подразделений организации	Руководитель подразделения задает тон отношения сотрудников к проблемам ИБ, которое, в свою очередь, определяет качество применяемых в подразделении защитных мер
	Недостаточная осведомленность персонала в области информационной безопасности	Отношение сотрудников к проблемам ИБ определяет качество применяемых в подразделении защитных мер
	Оперативность реагирования службы ИБ на изменения ИТ-среды	Реагирование включает прогнозирование предстоящих изменений, оценку и согласование состава и времени изменений с заинтересованными службами, а также активный поиск связанных с изменениями проблем безопасности
	Естественная изменчивость бизнеса организации, порождающая изменчивость технологических процессов	Многочисленные изменения повышают риски, поскольку ИТ-среда постоянно находится в «окне уязвимости»
	Значительное число изменений, вносимых в информационные системы организации и не связанных прямо с изменениями бизнеса организации	Многочисленные изменения повышают риски, поскольку ИТ-среда постоянно находится в «окне уязвимости». Изменения, не связанные с изменениями цели организации, являются необязательными, их можно избежать
	Наличие недостатков отображения технологического процесса на ИТ-инфраструктуру	ИТ-инфраструктура содержит избыточные структурные элементы, предполагает избыточные с точки зрения бизнеса операции, не удовлетворяет части бизнес-требований
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
7. Слабая детерминированность процессов основной деятельности организации. Возникновение необходимости реализации деятельности в организации за пределами регламентов, поскольку организация вынуждена искать различные способы реализовать цель в условиях изменчивой среды	Ошибки и сбои программных и аппаратных компонентов информационной системы	Нештатные и аварийные ситуации могут быть удобным прикрытием для нападения или сокрытия его следов
	Ошибки, совершаемые сотрудниками организации	Никто не застрахован от ошибок, но разные люди совершают их по-разному и в разных количествах, что связано как с индивидуальными особенностями человека, так и с условиями среды. Один из распространенных вариантов защитного поведения внутреннего злоумышленника при расследовании — интерпретация своих действий как ошибочных
	Возможность действий внутреннего злоумышленника, приводящих к нештатным и аварийным ситуациям	Нештатные и аварийные ситуации могут быть удобным прикрытием для нападения или сокрытия его следов. Легко представить сотрудника, обладающего возможностями и воображением, необходимыми для инсценировки аварии

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Нарушение функциональности средств защиты	Применяемые организацией защитные меры в силу различных причин могут бездействовать в течение некоторого периода рабочего времени — «окна» уязвимости. При этом риски соответственно повышаются
	Прогнозирование инсайдером возникновения нештатной или аварийной ситуации	Внутренний злоумышленник, даже не инсценируя аварию, может предсказать ее возникновение, подготовиться и воспользоваться результатом
	Недостаточная компетентность персонала	Отсутствие опыта, знаний или стремления к достижению качественного результата деятельности порождает массу скрытых и явных проблем, способствующих реализации преднамеренных угроз ИБ от персонала
	Несоответствие регламентов деятельности реальной операционной среде и процессам организации	Если сотрудник не может действовать по регламенту, он будет действовать, как считает необходимым. В этом случае становятся неэффективны многие защитные меры, а расследование инцидентов не позволит выявить виновника
	Халатность сотрудников организации	Способствует реализации преднамеренных угроз. Наряду с ошибкой может использоваться злоумышленником в качестве прикрытия преднамеренных действия
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
8. Неадекватность установленных отношений владения информационными активами	Сложность используемых организацией технологий обработки информации и информационных систем	Сложность связана с общей сложностью современных ИТ, а также со сложностью автоматизированных процессов организации
	Нарушение согласованности управления доступом к совместно используемым ресурсам в случае, когда владельцы и пользователи активов относятся к различным организационным подразделениям	Когда обмен информацией и потребностями затруднен в результате различной организационной подчиненности сотрудников, назначенные права доступа, как правило, избыточны по сравнению с необходимыми
	Проблемы в управлении организацией в целом или ее структурными подразделениями	В качестве примеров проблем можно привести несоответствие циклов улучшения организации темпу изменениям среды, неадекватное распределение ресурсов и т. п.
	Возможность конфликта интересов между подразделениями организации при осуществлении некоторых процессов ИБ (мониторинг, расследование инцидентов ИБ и др.)	Реализация защитных мер, на которых настаивает служба ИБ может оказаться нежелательной с точки зрения службы ИТ, а применение защитных мер может показаться неудобным пользователям
9. Сговор внешнего и внутреннего злоумышленников	Не аннулированные своевременно полномочия бывших сотрудников организации	Хотя политика ИБ зрелой организации предусматривает отзыв всех полномочий в случае увольнения сотрудника или даже перехода на другую должность, на практике такая операция может быть забыта, проведена с опозданием или проведена не полностью. Кроме того, почти всегда многие сотрудники не знают об увольнении коллеги и готовы предоставить ему информацию или выполнить иную просьбу
	Бывшие сотрудники, обладающие значительными знаниями	Уход сотрудника — зачастую это утечка (а порой и безвозвратная потеря) важной информации об особенностях операционной среды организации. Усугубляет ситуацию возможность его трудоустройства в конкурирующую организацию

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Поддержка действий внутреннего злоумышленника извне организации	Внешняя поддержка существенно может увеличить шансы внутреннего злоумышленника на успех, а организации — на увеличение ущерба. Внешняя поддержка часто заключается в обеспечении инсайдера ресурсами, обеспечении канала сбыта информации (или другого способа приобретения выгоды), инсценировке ситуаций, благоприятствующих осуществлению нападения
	Оказание давления на сотрудника организации внешними злоумышленниками тем или иным способом (угрозы близким сотрудника, угрозы в отношении имущественных или других прав сотрудника)	Внешнее принуждение делает возможным нападение даже со стороны самого благонадежного сотрудника
	Возможность приема на работу в организацию недостаточно благонадежных лиц	—
10. Кадровые проблемы (недостаточная лояльность и благонадежность персонала)	Кадровые изменения	Изменения состава сотрудников, реализующих некоторую деятельность, может повлиять как на качество результатов этой деятельности, так и на ее защищенность от угроз. Существенный риск связан с процессом «вхождения» каждого нового сотрудника в роль (должность), с получением сотрудником необходимых знаний, с неизбежными ошибками и т.д.
	Халатность сотрудников организации	Способствует реализации преднамеренных угроз. Наряду с ошибкой может использоваться злоумышленником в качестве прикрытия преднамеренных действия
	Неблагоприятный моральный психологический климат в коллективе организации	Возможен конфликт интересов на почве личной неприязни сотрудников. Отсутствие доверия между сотрудниками ухудшает информационные процессы. Возможно возникновение враждующих кланов внутри организации

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Неудовлетворенность персонала организации условиями труда, в частности, уровнем оплаты труда	Вероятно возникновение заинтересованности в дополнительном заработке, намерений смены работы
	Недостаточное осознание проблем ИБ руководителями структурных подразделений организации	Руководитель подразделения задает тон отношения сотрудников к проблемам ИБ, которое, в свою очередь, определяет качество применяемых в подразделении защитных мер
	Наличие у сотрудников индивидуальных особенностей, проблем и мотивов, способных при неблагоприятных условиях подтолкнуть сотрудника к действиям против интересов организации	—
	Возможность приема на работу в организацию недостаточно благонадежных лиц	—
	Высокая текучесть кадров	Свидетельствует о наличии кадровых проблем в организации. Высокие риски как с точки зрения защищенности, так и с точки зрения появления мотивированного внутреннего злоумышленника
11. Объективная неадекватность функциональности информационных систем организации требованиям бизнеса, в частности, избыточность функциональности информационных систем	Сложность используемых организацией технологий обработки информации и информационных систем	Сложность связана с общей сложностью современных ИТ, а также со сложностью автоматизированных процессов организации

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Неоднородность системных и прикладных платформ, используемых организацией	Технический и программный «зоопарк» создает многочисленные сложности как в управлении ИТ, так и в управлении ИБ организации
	Наличие недостатков отображения технологического процесса на ИТ-инфраструктуру	ИТ-инфраструктура содержит избыточные структурные элементы, предполагает избыточные с точки зрения бизнеса операции, не удовлетворяет части бизнес-требований
	Возможность отклонения хода технологического процесса от установленного порядка	Установленный порядок реализации технологического процесса не только содержит встроенные защитные меры, но и является условием успешного применения внешних по отношению к данному процессу защитных мер. Перевод технологического процесса (или его участка) в нештатный, ручной, аварийный режим всегда создает риски, в том числе связанные с персоналом
12. Злоупотребление доверием других сотрудников организации	Возможность использования внутренним злоумышленником полномочий и знаний других сотрудников в рамках служебных или неформальных отношений	Подобная ситуация — один из побочных эффектов атмосферы доверия к организации. Зачастую проще всего обмануть самых лучших и старательных сотрудников, поскольку они часто сконцентрированы на своей основной задаче и могут упустить из внимания факты, не относящиеся к такой задаче
	Ошибки, совершаемые сотрудниками организации	Никто не застрахован от ошибок, но разные люди совершают их по-разному и в разных количествах, что связано как с индивидуальными особенностями человека, так и с условиями среды. Один из распространенных вариантов защитного поведения внутреннего злоумышленника при расследовании — интерпретация своих действий как ошибочных
	Недостаточная компетентность персонала	Отсутствие опыта, знаний или стремления к достижению качественного результата деятельности порождает массу скрытых и явных проблем, способствующих реализации преднамеренных угроз ИБ от персонала

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Возможность завладения полномочиями других сотрудников, Возможность действия с их полномочиями и под их идентификатором	Наиболее привлекательным объектом для нападения, вероятно, являются атрибуты безопасности сотрудника, обладающего наибольшими полномочиями. Замаскированный таким образом злоумышленник не без оснований чувствует себя защищенным и весьма опасен
	Недостаточная осведомленность персонала в области информационной безопасности	Отношение сотрудников к проблемам ИБ определяет качество применяемых в подразделении защитных мер
	Действия организованной группы внутренних злоумышленников	Организованная группа имеет значительно больше возможностей реализовать цель в рамках штатных полномочий, чем злоумышленник-одиночка. Во-первых, полномочия и знания группы больше. Во-вторых, действия нескольких лиц гораздо труднее ассоциировать при мониторинге и расследовании. Таким образом, может быть достигнута более высокая скрытность. Группа злоумышленников может реализовать цель более высокого уровня, чем одиночка
13. Неопределенность в отношении адекватности принимаемого организацией риска, связанного с угрозами ИБ от персонала	Отсутствие оперативных действий по реагированию на инциденты	Отсутствие оперативных действий по реагированию на инцидент дает злоумышленнику преимущество во времени. Пользуясь таким преимуществом на этапе подготовке атаки, в случае неоперативного реагирования он получает преимущество в процессе проведения атаки и при последующем расследовании
	Отсутствие формализованных процедур обработки инцидентов	В каждом отдельном случае обработка инцидента будет организована стихийно, займет продолжительное время, а результат обработки инцидента с большой вероятностью окажется более низкого, чем возможно, качества

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Задержка получения службами ИТ и ИБ организации сведений об уязвимостях информационных систем организации	Производители ПО стараются сдержать распространение информации о выявленной уязвимости хотя бы до момента выпуска закрывающих ее «заплаток». При этом все равно существует круг лиц (разработчики, тестировщики, эксперты по ИБ), которым известно о наличии и особенностях уязвимости. Таким образом, существует период времени, когда факт уязвимости некоторого компонента системы службе ИБ не известен, но известен другим лицам
	Медленное распространение «заплаток», устраняющих известные уязвимости компонентов информационных систем	Устранение ошибок в ПО — сложный и ресурсоемкий процесс, особенно для ключевых компонентов информационной системы. «Заплатки» доходят до службы ИТ организации с существенной задержкой относительно обнаружения уязвимостей. При этом эксплуатируемое ПО все время до установки «заплатки» является уязвимым
	Слабости технических и организационных мер защиты информации, применяемых организацией	Состав применяемых защитных мер и их слабости обычно хорошо известны сотрудникам и зачастую в нарушение действующих политик ИБ используются для «упрощения» работы
	Недостатки применяемых в организации процедур накопления знаний по проблемам и инцидентам	Нежелательные для организации последствия связаны с тем, что фрагменты знаний будут накапливаться только у отдельных людей — участников обработки инцидентов, не будут распространяться и накапливаться в организации
	Уязвимости программных и аппаратных компонентов информационной системы	Уязвимости системных, прикладных компонентов информационной системы, а также средств защиты информации позволяют внутреннему злоумышленнику действовать за пределами своих служебных полномочий

Продолжение табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Возможность преодоления защитных мер, ограничивающих полномочия сотрудников	В отличие от внешнего злоумышленника инсайдер обладает более высокими шансами на преодоление защитных мер, поскольку обладает необходимым временем, базовыми полномочиями доступа (физическим, сетевым), знаниями, а также пользуется доверием со стороны организации
	Невозможность централизованного управления полномочиями сотрудников	В условиях распределенного управления полномочиями единой картиной распределения полномочий никто в организации не обладает
	Наличие уязвимостей в технологических процессах организации	Уязвимости в технологических процессах (недостатки распределения ролей, наличие альтернативных путей процесса без четких условий их выполнения, другие неопределенности) позволяют внутреннему злоумышленнику вмешаться в ход технологического процесса (с использованием полномочий или без них), реализуя свою цель
	Несоблюдение нормативно-распорядительных документов организации	Наличие норм не означает автоматического их выполнения персоналом. Массовое несоблюдение установленных организацией норм может быть как результатом слабой исполнительской дисциплины, так и низкого качества самих норм
	Возможность влияния инсайдера на решения, принимаемые службой ИБ организации	Злоумышленник постарается обосновать и ввести ограничения на осуществление отдельных процессов ИБ или реализацию важных защитных мер (регистрация, мониторинг, ограничение доступа и др.)
	Неадекватность модели угроз ИБ от персонала	Результатом является неправильное позиционирование защитных мер
	Несогласованность применения различных защитных мер ИБ	Возможно возникновение уязвимостей на стыках защитных мер разного типа, совместно применяемых различными подразделениями, зависимых друг от друга защитных мер

Окончание табл. 12

Фактор первого уровня	Фактор второго уровня	Пояснение к фактору второго уровня
	Деградация комплекса защитных мер со временем	Комплекс защитных мер, а также их настройки обычно отстают от развития защищаемой информационной системы, что является причиной снижения уровня защищенности
	Юридические сложности, связанные с наказанием внутренних злоумышленников и других внутренних нарушителей ИБ	Сложности могут возникнуть как при квалификации действия внутреннего злоумышленника, так и при обеспечении производства юридически значимыми свидетельствами
	Неадекватная оценка рисков, связанных с угрозами ИБ от персонала	Такой недостаток ведет к неадекватности определения целей и приоритетов ИБ в области противодействия угрозам ИБ от персонала
	Сложность прогнозирования действий внутреннего злоумышленника	Объективная неопределенность, связанная с тем, что организация прогнозирует нападение, исходящее из внутренней, доверенной среды

Как было отмечено выше, перечисленные выше факторы первого и второго уровня образуют систему причинно-следственных отношений. Возможные отношения между факторами показаны на примере фрагмента сети факторов риска ИБ от персонала, представленном на рис. 64.

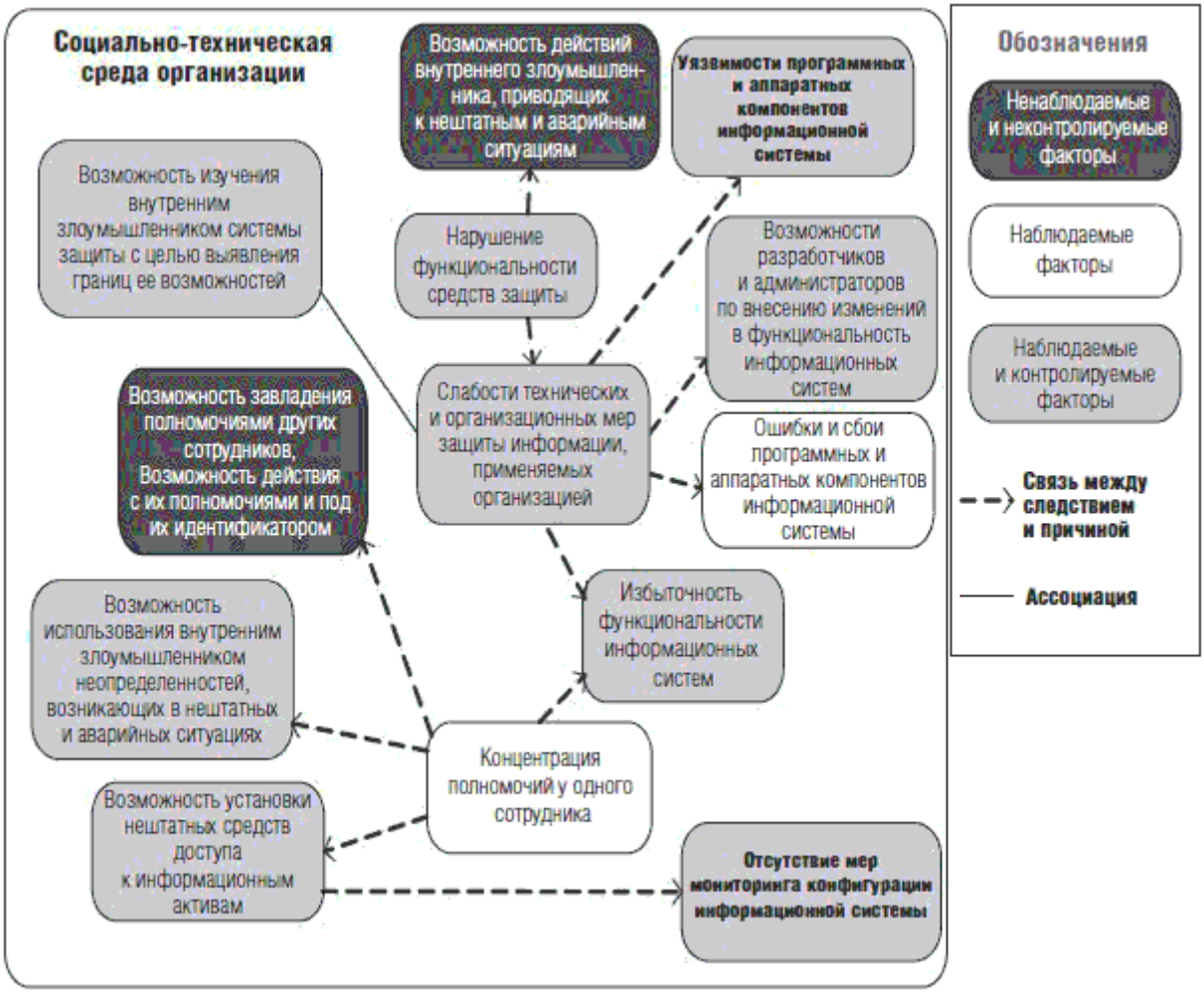


Рис. 64. Фрагмент сети факторов риска ИБ от персонала

Все факторы системы сплетены в огромную причинно-следственную сеть, в которой есть скрытая от наблюдения менеджмента организации часть и наблюдаемая часть. Понятно, что с точки зрения предлагаемой модели повышение защищенности в отношении угроз ИБ от персонала может быть достигнуто путем оценки и контроля со стороны организации факторов риска второго уровня. Предложенную нами систему факторов можно использовать именно таким способом, реализуя следующий план действий:

– определить состав наблюдаемых факторов и внедрить способы их измерения;

– определить состав контролируемых факторов и установить механизмы контроля;

– организовать при помощи созданных механизмов систему контроля рисков ИБ, связанных с персоналом;

– осуществлять при помощи созданной системы контроля последовательные мероприятия по приведению рисков ИБ от персонала в соответствие ожидаемому уровню.

4.2.4. Некоторые модели угроз

Разнообразие угроз ИБ от персонала позволяет построить не менее разнообразные модели. Например, пространство возможной вины участника инцидента показано на рис. 65 в двух измерениях:

– по вертикальной оси – «стремление к последствиям нападения», которое изменяется от нежелательности последствий инцидента с точки зрения инсайдера до сознательного стремления инсайдера нанести наибольший ущерб организации и другим вовлеченным в инцидент лицам;

– «предвидение последствий», которое изменяется от субъективной неспособности

(или объективной невозможности) сотрудника предвидеть негативные последствия своих действий до уверенного предвидения неизбежности инцидента и его негативных последствий.

Рис. 65. Модель умысла участника инцидента

В предложенном пространстве вины могут быть размещены все происходящие в организации инциденты, хотя сделать это может быть и не просто. Собранная на подобном рисунке статистика организации за период времени покажет, в каком направлении работы с персоналом необходимо вести профилактические мероприятия.

Модель возможностей сотрудников [34] как важной составляющей их опасности для организации приведена на рис. 66.

Это модель демонстрирует связь между опасностью сотрудника (с точки зрения его возможностей по реализации атаки) и его ролью в информационной системе организации.

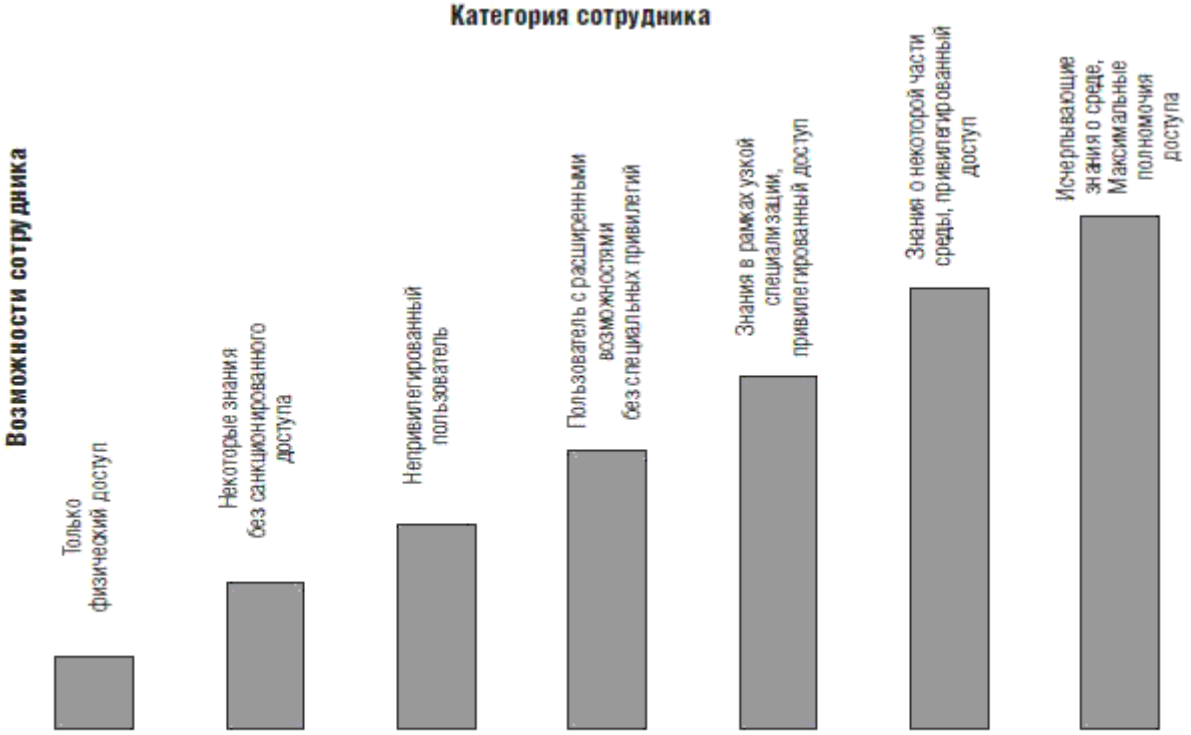


Рис. 66. Модель возможностей сотрудников

Модель поведения внутреннего злоумышленника применительно к инциденту с утечкой информации «на заказ», представлена на рис. 67.

Часть действий внутреннего злоумышленника (светлые области на рисунке) является ненаблюдаемой для организации, другая часть наблюдаема при осуществлении организацией целенаправленной деятельности по повышению обзора по соответствующим направлениям.

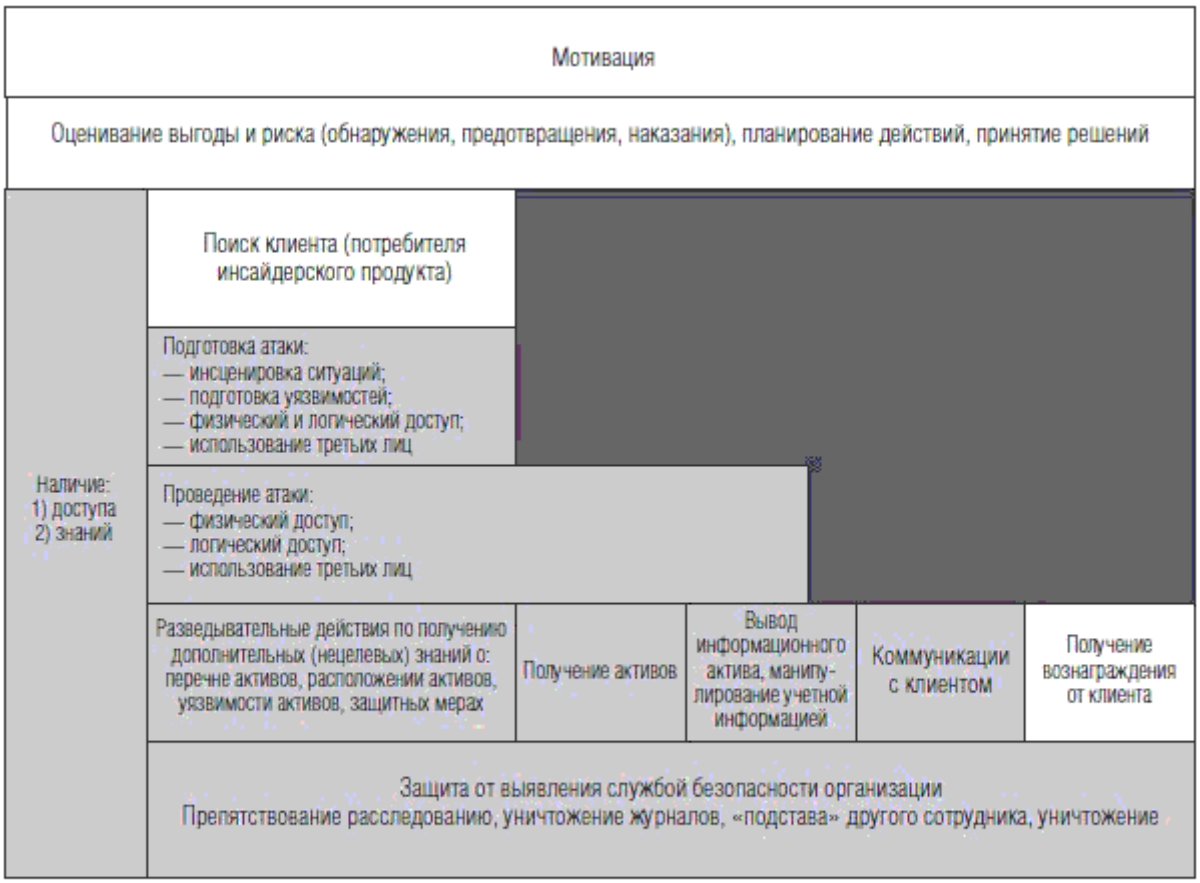


Рис. 67. Модель поведения внутреннего злоумышленника применительно к инциденту с утечкой информации

4.2.5. Внешние сообщники внутреннего злоумышленника

Высока вероятность действий внутреннего злоумышленника в сговоре с внешним по отношению к организации лицом (внешним злоумышленником). При этом инсайдер может выступать как организатором нападения, так и используемым внешней силой в своих целях исполнителем или пособником нападения. «Свой человек» в организации почти всегда может оказаться полезен внешним злоумышленникам.

Виды сотрудничества инсайдера с внешней силой разнообразны, он может выступать:

– организатором нападения;

– используемым «вслепую» (например, путем обмана) помощником;

– полностью манипулируемым (например, путем подкупа или шантажа) агентом;

– самостоятельным агентом (реализующим собственную цель помимо внешней злоумышленной);

– поддерживаемым агентом (реализующим только собственную цель, однако пользующимся внешней поддержкой).

Пособническая поддержка, оказываемая внутреннему злоумышленнику внешним сообщником, может включать:

– финансовые ресурсы;

– специализированные технические средства;

– инсценировку событий, облегчающих осуществление различных шагов атаки;

– информационное и аналитическое обеспечение;

– правовую помощь;

– содействие в сокрытии следов;

– содействие в сбыте похищенных информационных активов или легализации приобретенных материальных выгод.

4.2.6. Типология мотивов

Противоправное поведение внутреннего злоумышленника может быть результатом действия сложного сочетания нескольких мотивов из следующего (не исчерпывающего) перечня (см., например, [52]):

– корыстный интерес (приобретение материальной выгоды);

– принуждение со стороны третьих лиц;

– личная заинтересованность, связанная с родственными и иными близкими отношениями или определенными обязательствами перед сторонними лицами;

– месть;

– самоутверждение;

– любопытство;

– игровой мотив (стремление к острым ощущениям, авантюризм);

– искаженное чувство справедливости;

– стремление любой ценой выполнить должностные обязанности;

– карьеризм;

– хулиганские побуждения;

– зависть;

– идеологические соображения;

– вражда;

– стремление субъекта скрыть компрометирующие его факты (нарушения, информацию о себе или близких);

– неудовлетворенность различными аспектами личной жизни или трудовых отношений;

– наркотическая или алкогольная зависимость.

Кроме того, важны различные особенности личности инсайдера, например, следующие (см., например, [33]):

– безразличие субъекта к собственным рискам, возникающим при совершении нарушения;

– уверенность в том, что нарушение не будет выявлено;

– уверенность в том, что возможное наказание не будет адекватным;

– привычка действовать определенным образом;

– самооправдание;

– жестокость;

– трусость;

– нерешительность.

4.2.7. Сговор

Данный тип умышленных инцидентов является весьма опасным, хуже выявляется и наносит большие негативные последствия по сравнению с другими инцидентами, хотя и встречается значительно реже остальных.

Сговор инсайдеров является менее вероятным событием, чем деятельность внутреннего злоумышленника в одиночку. Сговор инсайдеров расширяет круг возможностей злоумышленной деятельности, вследствие чего ущерб от атаки может быть значительно больше, чем от атаки злоумышленника-одиночки, а возможности организации по предотвращению, выявлению и пресечению атаки и выявлению внутреннего

злоумышленника могут оказаться снижены.

4.2.8. Деятельность внутреннего злоумышленника с точки зрения формальных полномочий

По отношению к правовой базе организации, определяющей служебные полномочия сотрудников, каждое действие внутреннего злоумышленника в ходе происшествия можно отнести к одному из следующих типов:

– действие в рамках служебных полномочий;
– злоупотребление служебными полномочиями;
– превышение служебных полномочий;
– действия в сфере неопределенных служебных полномочий.

Управление идентификационными данными и доступом *(IBM Восточная Европа/Азия)*

Краткий обзор

В современной конкурентной среде глобального бизнеса информация доставляется быстрее, новые продукты выводятся на рынок оперативнее. Разрабатываются новые, усовершенствованные и более конкурентоспособные модели ведения бизнеса. Чтобы оперативно реагировать на непрерывно меняющиеся потребности и возможности, а также адаптироваться к ним, бизнесу необходимо обеспечить достаточную гибкость и поддержку взаимодействий между людьми и компаниями. Сотрудники должны быстрее получать доступ к значимой информации, а также иметь возможности для эффективной совместной работы. Отдельные специалисты и коллективы должны работать так, как им удобно, в любое время, где бы они ни находились.

Однако удовлетворение потребностей в более динамичном сотрудничестве и свободном доступе к ресурсам значительно усложняет задачи обеспечения безопасности и выполнения нормативных требований – в особенности в условиях растущего количества сотрудников, работающих в мобильном режиме. Организациям необходимо связывать клиентов, партнеров и поставщиков с множеством корпоративных систем и процессов. Чтобы упростить выполнение регулирующих норм и гарантировать конфиденциальность, целостность и доступность своих данных, приложений и систем, организации должны удостовериться в том, что доступ к ресурсам предоставляется только тем пользователям, которые имеют на это право, применять средства контроля доступа, а также обеспечивать мониторинг событий в системе безопасности с формированием соответствующих отчетов.

К сожалению, традиционные решения для обеспечения безопасности реализуют подход «снизу вверх», который позволяет исключать отдельные проблемы путем развертывания точечных решений, основывающихся на использовании отдельных политик и процессов. Применение подобного подхода приводит к росту сложности, излишним затратам, неэффективному использованию ресурсов, пробелам в системе безопасности и изолированности данных, что оказывает негативное влияние на продуктивность компании и ее сотрудников.

Организациям требуется единый, целостный подход к обеспечению безопасности, в рамках которого инициативы по защите корпоративной среды согласуются с целями бизнеса. Такой подход «сверху вниз» позволяет эффективно использовать методы обеспечения безопасности для защиты и совершенствования бизнес-процессов и коллективной работы. Однако подобная методика должна предполагать модульную реализацию плана, чтобы организации могли сконцентрироваться в первую очередь на наиболее значимых областях.

Ключевые моменты

По мнению отраслевых аналитиков, в десятку самых серьезных угроз корпоративной безопасности входят ошибки сотрудников, кражи данных сотрудниками и бизнес-партнерами, а также злонамеренные действия инсайдеров.

Основываясь на глубоком понимании внутренних и внешних угроз корпоративной безопасности, IBM предлагает адаптируемый, соответствующий потребностям бизнеса, целостный подход к обеспечению безопасности.

Такой подход охватывает различные области рисков, оказывающих влияние на состояние системы безопасности в организации:

• Пользователи и идентификация – предоставлять пользователям в организации и за ее пределами, включая поставщиков, партнеров и клиентов, свободный доступ к необходимым данным и инструментам, блокируя доступ для тех, у кого нет такой необходимости или нет соответствующих прав.

• Данные и информация – поддерживать масштабное сотрудничество по электронным каналам, защищая важнейшие данные при их передаче и хранении.

• Приложения – обеспечивать эффективную защиту важнейших для бизнеса приложений и процессов от внешних и внутренних угроз в течение всего жизненного цикла, от проектирования до развертывания и эксплуатации.

• Сеть, серверы и конечные точки – поддерживать эффективный мониторинг сети, серверов и конечных точек, обеспечивая безопасность организации в условиях растущего количества угроз и уязвимостей.

• Физическая инфраструктура – защищать ИТ-активы с использованием средств контроля физического доступа, а также обеспечивать защиту физических активов от различных угроз для повышения уровня безопасности в целом.

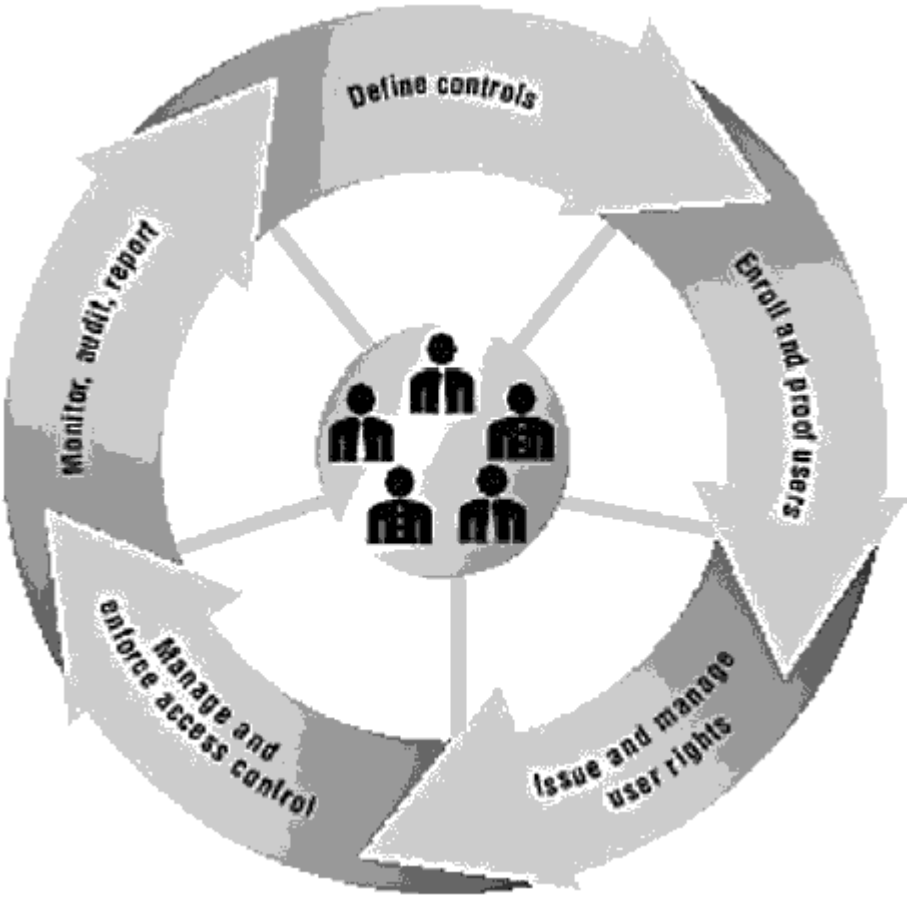
В составе своей полнофункциональной структуры обеспечения безопасности IBM предлагает обширный, интегрированный комплекс решений для управления доступом и идентификационными данными. Это помогает организациям укреплять безопасность коллективной работы и доступа к ресурсам в соответствии с потребностями бизнеса.

Эффективное использование подхода на базе стандартов к управлению жизненным циклом идентификационных данных и доступом в соответствии с потребностями бизнеса

Развитие информационных технологий всегда поддерживалось инновациями. Реализация новых идей позволяет более эффективно собирать и совместно

использовать информацию в масштабе всего предприятия. Однако применение новых способов обмена и использования информации сопровождается появлением новых потенциальных угроз корпоративной безопасности – не только внешних, но и внутренних. По мнению отраслевых аналитиков, в десятку самых серьезных угроз корпоративной безопасности входят ошибки сотрудников, кражи данных сотрудниками и бизнес-партнерами, а также злонамеренные действия инсайдеров.

Для решения этих важнейших проблем безопасности и бизнеса IBM предпринимает основанный на стандартах и определяемый потребностями бизнеса подход к управлению идентификационными данными и доступом, который охватывает весь жизненный цикл информационных и физических активов. Такой подход интегрирует управление авторизацией и идентификационными данными, чтобы предоставить организациям возможность экономически эффективно защищать активы и информацию, поддерживая динамичную коллективную работу и оперативный доступ к ресурсам для повышения продуктивности бизнеса. Этот воспроизводимый процесс позволяет организациям управлять рисками для множества бизнес-инициатив, обеспечивая сокращение затрат, предлагая пользователям более комфортные условия для работы, повышая эффективность бизнеса и рационализируя деятельность по выполнению нормативных требований. Он поддерживает соблюдение требований таких нормативных актов и стандартов, как Закон Сарбейнса-Оксли (Sarbanes-Oxley, SOX), Payment Card Industry (PCI), Basel II, закон EU Data Protection о защите персональной информации и Закон об использовании и защите сведений о пациентах (Health Insurance Portability and Accountability Act, HIPAA).



Пять основных этапов жизненного цикла управления идентификационными данными и доступом:

- определение средств контроля;
- регистрация и проверка пользователей;
- управление правами пользователей;
- контроль доступа;
- мониторинг, аудит и составление отчетов о правах и действиях пользователей.

Жизненный цикл управления идентификационными данными и доступом	
Определение средств контроля	IBM Identity Assessment and Strategy Services IBM Tivoli Identity and Access Management
Регистрация и проверка пользователей	IBM Identity Resolution IBM Relationship Resolution
Управление правами пользователей	IBM Tivoli Identity Manager IBM Tivoli Directory Server IBM Tivoli Directory Integrator IBM Tivoli zSecure suite with RACF®
Контроль доступа	IBM Tivoli Access Manager IBM Tivoli Federated Identity Manager IBM Tivoli zSecure suite with RACF
Мониторинг, аудит и составление отчетов о правах и действиях пользователей	Tivoli Identity Manager Tivoli Security Information and Event Manager

В следующих разделах эти пять основных этапов описываются более подробно.

Определение средств контроля

Эффективное управление идентификационными данными и доступом начинается не с инструментов и технологий, а с определения необходимых средств контроля и связанных процессов.

Ключевые моменты

Определив необходимые средства контроля и процессы в начале жизненного цикла идентификационных данных, организации смогут разработать эффективные политики обеспечения безопасности в соответствии с приоритетами бизнеса.

На этом этапе решения IBM для управления идентификационными данными и доступом позволяют организациям определить средства контроля и процессы на базе соответствующих стандартов, правовых и регулирующих норм, а также потребностей и целей бизнеса. Организации должны оценить требования бизнес-среды к идентификационным данным, определить ресурсы, требующие контроля доступа, пользователей и группы пользователей, которым необходимо предоставлять доступ к ресурсам, а также тип предоставляемого доступа. Определив необходимые средства контроля и процессы в начале жизненного цикла идентификационных данных, организации смогут разработать эффективные политики обеспечения безопасности в соответствии с приоритетами бизнеса.

Регистрация и проверка пользователей

Решения IBM для управления идентификационными данными и доступом позволяют организациям анализировать идентификационные данные в точках контакта и выявлять взаимосвязи до того, как станет слишком поздно блокировать нелегитимный доступ пользователя. Эти решения помогают определить, кто есть кто, и обнаружить взаимосвязи между пользователями. Организациям предоставляются методики анализа объектов,

позволяющие обнаруживать явные и неявные взаимосвязи в реальном времени. Взаимосвязи могут быть раскрыты, даже если пользователи в сети пытаются скрыть или исказить свои идентификационные данные. Кроме того, организации могут в момент регистрации обеспечивать анализ потоков данных из множества источников.

Управление правами пользователей

Помимо определения соответствующих учетных записей и прав для пользователей и групп пользователей решения IBM для управления идентификационными данными и доступом предоставляют организациям эффективные средства поддержки актуальности учетных записей, включая добавление, обновление, проверку соответствия и удаление прав по мере изменения потребностей пользователей в получении доступа.

Организации могут:

• оперативно определять идентификационные данные и права и управлять ими на протяжении всего жизненного цикла;

• легко обнаруживать и удалять устаревшие учетные записи, чтобы блокировать доступ к информации и ресурсам для бывших партнеров и сотрудников;

• сопоставлять учетные записи с идентификационными данными, а также проверять права доступа посредством подтверждения необходимости дальнейшего предоставления их пользователю;

• предоставлять пользователям возможность самостоятельно восстанавливать свои пароли, исключая задержки и сокращая затраты службы поддержки пользователей.

Контроль доступа

Мониторинг действий пользователей является необходимым условием эффективного контроля доступа. Решения IBM для управления идентификационными данными и доступом предоставляют платформу для централизованного управления политиками доступа, позволяющую поддерживать требуемый уровень прозрачности, а также проще обеспечивать безопасность и выполнение регулирующих норм. Кроме того, организации могут контролировать предоставление пользователям доступа к разрешенным ресурсам, удостоверяться в том, что пользователи являются теми, кем представляются, и ограничивать действия пользователей только теми, на которые они имеют право, в различных приложениях и сервисах. Повышение продуктивности пользователей обеспечивает автоматизация предоставления доступа на основе механизма однократной регистрации (Single Sign-On, SSO). Кроме того, организациям, развертывающим сервисно ориентированные архитектуры (SOA), необходимо связывать множество учетных записей пользователей в рамках составных SOA-транзакций, а также справляться с возможными сложностями управления и соблюдения регулирующих норм. Функции управления идентификационными данными и доступом в решении IBM WebSphere® Enterprise Service Bus позволяют организациям сопоставлять, распространять и проверять идентификационные данные пользователей для различных систем аутентификации.

Мониторинг, аудит и составление отчетов о правах и действиях пользователей

Чтобы удостовериться в том, что существующие средства контроля и политики способны защитить важнейшие бизнес-приложения и конфиденциальную информацию, организациям необходима возможность поддерживать непрерывный мониторинг, аудит и формирование отчетов о правах и действиях пользователей. Решения IBM для управления идентификационными данными и доступом предоставляют такую возможность, позволяя организациям убедиться в том, что они должным образом защищены. Такие решения обеспечивают аудит и подготовку отчетов о соблюдении регулирующих норм и позволяют

непрерывно совершенствовать средства контроля над идентификационными данными.

Защита бизнес-систем и информации с использованием решений для управления идентификационными данными и доступом

Основой любой корпоративной стратегии информационной безопасности является способность обеспечивать аутентификацию и авторизацию пользователей. Понятие «легитимный пользователь» расширяется, и теперь оно включает не только сотрудников предприятия, но и его партнеров и клиентов, поэтому задача управления идентификационными данными и доступом становится более сложной. Появляются все новые угрозы для корпоративной инфраструктуры и ценной корпоративной информации.

Ключевые моменты

Решения IBM поддерживают мониторинг действий пользователей для соблюдения корпоративных политик управления безопасностью.

Решения IBM рационализируют управление жизненным циклом учетных записей и позволяют проще обеспечивать строгий контроль над доступом к ресурсам, разрешенным для пользователей. Кроме того, решения IBM поддерживают мониторинг действий пользователей для соблюдения корпоративных политик управления безопасностью, позволяя организациям проще подтверждать наличие эффективной среды контроля. IBM является ведущим поставщиком решений для управления учетными записями и web-доступом, неизменно входя в сектор лидеров «Магического квадранта» Gartner для этого рынка.

Авторизация пользователей

Авторизация должна обеспечивать оперативный доступ к ресурсам на протяжении всего жизненного цикла учетных записей – для множества сред, областей рисков, информационных процессов, приложений, сетей, конечных точек и всей физической инфраструктуры. При этом необходимо обеспечивать безопасность и защищать ИТ-среду от внутренних и внешних угроз, а также соблюдать нормативные требования. Поэтому решение для управления доступом должно обеспечивать:

- централизованный контроль, чтобы гарантировать выполнение политик безопасности для множества приложений и пользователей;
- автоматизацию с использованием инфраструктуры безопасности на базе политик, соответствующую ИТ-потребностям и целям бизнеса;
- однократную регистрацию для доступа к локальным, удаленным и web-системам, а также средства управления идентификационными данными и контроля доступа для сведения к минимуму проблем, связанных с паролями, – таких как путаница с использованием множества паролей, угрозы безопасности, вызванные тем, что пользователи записывают свои пароли, простои в работе в связи с блокированием учетных записей, а также необходимость уделять значительное время администрированию паролей;
- интегрированное управление доступом и идентификационными данными в одной инфраструктурной среде;
- совместное использование идентификационных данных пользователей различными приложениями на базе web-сервисов.

Для удовлетворения этих потребностей IBM предлагает услуги Identity and Access Management и ПО IBM Tivoli® Access Manager for e-business. Выполняя функции концентратора данных об аутентификации и авторизации для приложений разных типов, Tivoli Access Manager for e-business централизует управление безопасностью. Эта система позволяет проще и при меньших затратах развертывать надежные приложения.

Решение IBM Tivoli Access Manager for Enterprise Single Sign-On предлагает простые средства аутентификации для приложений разных типов, обеспечивая автоматизацию процесса однократной регистрации, укрепление безопасности благодаря автоматизированному управлению паролями, сокращение затрат службы поддержки пользователей и совершенствование средств аудита и подготовки отчетов.

Решение IBM Tivoli Access Manager for Operating Systems защищает ресурсы приложений и операционных систем, обеспечивая детализацию доступа для всех учетных записей в UNIX® и Linux®, включая учетные записи superuser и root.

Решение IBM Tivoli Federated Identity Manager позволяет клиентам, поставщикам и партнерам безопасно, гибко и эффективно вести бизнес в различных средах и множестве доменов безопасности. Предлагая простую, свободно связываемую модель управления идентификационными данными и доступом к ресурсам, решение Tivoli Federated Identity Manager также позволяет сократить расходы на интеграцию, затраты службы поддержки пользователей, а также расходы на администрирование системы безопасности с использованием простого, оперативно развертываемого решения для однократной регистрации. Кроме того, IBM Tivoli Federated Identity Manager Business Gateway предлагает небольшим и средним организациям возможность развертывать федеративные средства однократной регистрации для доступа к web-ресурсам, чтобы сводить вместе клиентов, партнеров и поставщиков, с использованием одного, простого в развертывании приложения.

Для сред на базе SOA и web-сервисов решение Tivoli Federated Identity Manager предлагает надежные средства управления, обеспечивающие безопасный доступ к ресурсам мейнфрейма и распределенным сервисам. Например, это решение обеспечивает надежную защиту с использованием токенов и сопоставление идентификационных данных из множества источников и доменов безопасности.

Чтобы предоставить организациям возможность контролировать поведение пользователей в масштабе всей инфраструктуры, решение IBM Tivoli Security Information and Event Manager предлагает информационные панели, демонстрирующие статус соблюдения требований корпоративной безопасности, со средствами углубленного мониторинга действий привилегированных пользователей и полным набором функций ведения регистрационных журналов и аудита.

Управление идентификационными данными

Для эффективного обеспечения безопасности требуется управление идентификационными данными пользователей и их правами доступа к ресурсам на протяжении всего жизненного цикла учетных записей. Интегрированное решение должно охватывать ключевые области управления идентификационными данными:

- управление жизненным циклом идентификационных данных, включая самообслуживание, регистрацию и предоставление прав доступа;
- контроль идентификационных данных, включая контроль доступа и конфиденциальности, а также однократную регистрацию и аудит.

Чтобы удовлетворить эти потребности, IBM предлагает решение Tivoli Identity Manager для автоматизированного управления пользователями на базе политик с обширными возможностями обеспечения безопасности. Это решение позволяет эффективно управлять учетными записями пользователей (а также разрешениями на доступ и паролями) – от создания до удаления, для всей ИТ-среды.

В развертывании, интеграции и использовании каталогов организациям помогут решения IBM Tivoli Directory Server и IBM Tivoli Directory Integrator. Эти базовые компоненты среды управления идентификационными данными предлагают масштабируемый, основанный на стандартах метод хранения данных о пользователях и синхронизации разрозненных источников этих данных в масштабе всего предприятия.

Услуги IBM Identity and Access Management Services помогают организациям оценивать, проектировать, развертывать и администрировать интегрированные решения для управления идентификационными данными на базе технологий IBM и ее бизнес-партнеров. Эти услуги могут поддерживать организации на всех этапах управления жизненным циклом идентификационных данных.

Ключевые моменты

IBM предлагает полный набор решений и услуг, позволяющих организациям реализовать единый, основывающийся на потребностях бизнеса подход к обеспечению безопасности.

Обширный ассортимент услуг IBM

Служба IBM Identity and Access Management Services предлагает обширный набор услуг, включая консалтинг и техническую поддержку, чтобы помочь клиентам справиться с проблемами защиты все более сложной корпоративной среды, сократить затраты на управление и максимально упростить внедрение политики обеспечения безопасности.

Эксперты IBM помогут вам разработать эффективные политики управления рисками и обеспечить соблюдение этих политик. В сотрудничестве со своими бизнес-партнерами IBM предлагает решения для строгой многофакторной аутентификации, в том числе основывающиеся на использовании смарт-карт, технологий биометрии и контроля доступа на базе ролей.

Защита и совершенствование коллективной работы и доступа к ресурсам

Основываясь на глубоком понимании сегодняшних угроз – и своем более чем 40-летнем лидерстве на рынке технологий обеспечения информационной безопасности, IBM предлагает полный набор решений и услуг, позволяющих организациям реализовать единый, ориентированный на потребности бизнеса подход к защите корпоративных ресурсов. Разработав структуру всестороннего обеспечения безопасности, IBM помогает организациям управлять всеми рисками нарушения ИТ-безопасности с целью их ослабления, предлагая технологии и экспертные знания, необходимые для развертывания решений, соответствующих уникальным потребностям бизнеса и приоритетам каждой организации.

Модульная, интегрированная структура обеспечения безопасности IBM предоставляет организациям возможность в первую очередь сконцентрироваться на своих самых неотложных проблемах, распространяя инициативы по обеспечению безопасности на другие области по мере необходимости. Для обеспечения безопасности коллективной работы и доступа к ресурсам в соответствии с целями бизнеса IBM предлагает обширный, унифицированный набор решений и услуг в области управления идентификационными данными и доступом. Эти решения призваны защитить активы и информацию от неавторизованного доступа, что повышает продуктивность и динамичность бизнеса.

Дополнительная информация

Чтобы узнать больше о решениях IBM, помогающих обеспечить безопасность коллективной работы и доступа к ресурсам в соответствии с потребностями бизнеса, или о различных инфраструктурах обеспечения безопасности, предлагаемых IBM, которые помогают защитить и усовершенствовать ваши бизнес-операции, свяжитесь с региональным представителем или бизнес-партнером IBM или посетите сайт ibm.com/ itsolutions/ security.

О решениях IBM Service Management

Решения IBM Service Management помогают организациям обеспечивать высококачественное, эффективно управляемое и непрерывное обслуживание, безопасное для пользователей, клиентов и партнеров. Организации любого масштаба могут эффективно использовать оборудование, программное обеспечение и услуги IBM для планирования, реализации и администрирования инициатив по управлению сервисами и активами, обеспечению безопасности и устойчивости бизнеса. Гибкие, модульные решения, поддерживающие управление бизнесом, развитие ИТ-инфраструктуры и ИТ-операции, основываются на многолетнем опыте сотрудничества с клиентами, лучших отраслевых методиках и технологиях на базе открытых стандартов. IBM является для клиентов стратегическим партнером, который помогает развертывать решения, обеспечивающие ускоренную окупаемость инвестиций и поддерживающие успешное развитие бизнеса.

ИБМ Восточная Европа/Азия Россия, 123317, Москва,
Пресненская наб., 10
Тел.: 7 (495) 775-8800,
7 (495) 940-2000 Факс: 7 (495) 940-2070
E-mail: info@ru.ibm.com
ibm.com.ru

4.3. Противодействие угрозам ИБ от персонала

4.3.1. Общий подход к противодействию

В предыдущих разделах мы дали общую характеристику угроз ИБ от персонала и привели некоторые модели таких угроз. В данном разделе приводятся рекомендации по организации комплексного противодействия угрозам ИБ от персонала.

Далее сформулированы некоторые тезисы относительно противодействия угрозам ИБ от персонала.

Рисков ИБ от персонала невозможно полностью избежать, поэтому организация должна выявлять, оценивать и снижать соответствующих риски, признавать и принимать остаточный риск.

Установить тотальный контроль за действиями сотрудников невозможно, поэтому защитные меры должны быть избирательными.

Любые защитные меры тратят ресурсы организации в разной форме – человеко-часах, денежных единицах, доверии в коллективе и т. д. Поэтому любая система защитных мер должна быть сбалансирована по стоимости с потерями от возможного инцидента.

Любая система защитных мер не безупречна, в этой связи необходимо проводить контрольные и оценочные мероприятия в отношении применяемых защитных мер.

Как было отмечено в первом разделе главы, природа угроз от персонала не является новой. Поэтому целесообразно применять общеизвестные и проверенные многолетней практикой методы обеспечения доверия к персоналу, основанные прежде всего на информированности организации о сотруднике (принцип «знай своего служащего»).

Работа должна проводиться не только на этапе подбора сотрудника, но и на протяжении всей его работы. Кроме того, необходимо задуматься и о том, что будет после увольнения.

Акценты в выбранном подходе к противодействию угрозам от персонала создают специфику организации (некоторые организации сосредоточены на подборе персонала, другие – на ограничениях и контроле). Скорее всего, компания, занимающаяся розничной торговлей, выберет иные приоритеты, чем исследовательская лаборатория. Более того, в разных подразделениях одной организации тоже может быть целесообразно использовать различные подходы.

Большая часть защитных мер неизбежно связана с установкой различного рода ограничений на выполнение персоналом действий при выполнении служебных обязанностей. В этом случае решается задача о достаточности предоставленных полномочий для эффективного решения сотрудником служебных задач.

Общие подходы к оценкам в ИБ, изложенные в главе 3, могут быть успешно применены и к угрозам ИБ от персонала. Однако необходимо отметить, что в случае угроз от персонала оценки не могут быть очень точными, поскольку многие факторы не наблюдаемы, а для других факторов не существует объективных способов измерения (в том числе способов, которые возможно применять регулярно), но измерения могут дать ориентировочную, верную в первом приближении картину, позволят сравнить ситуации в организации, относящиеся к разным периодам, а также ситуации в разных организационных структурах, например региональных филиалах одной организации.

Оценочную модель для угроз ИБ от персонала можно строить, исходя из предложенной выше факторной модели угроз.

4.3.2. Обеспечение осведомленности персонала в области ИБ

Персонал должен знать о ценности информационных активов организации и потенциальных опасностях, занимать активную позицию в отношении защиты активов организации, не замалчивать проблемы и инциденты, внимательно относиться к подозрительным ситуациям, не стесняться задавать вопросы и информировать ответственную службу организации при необходимости. Обеспечить такие качества социума организации очень непросто, но это позволит в разы снизить вероятность возникновения инцидента при отсутствии грубых упущения по направлениям противодействия, не связанным с обеспечением осведомленности персонала.

М. Комер, автор книги «Расследование корпоративного мошенничества» [53], утверждает: «Один из лучших способов предотвращения внутреннего мошенничества – когда добропорядочные люди задают правильные и своевременные вопросы».

Целью организации должно быть создание и поддержание в коллективе культуры безопасности, атмосферы нетерпимости к нарушениям, когда нарушения не покрываются, а афишируются, наказываются, считаются позорными проявлениями непрофессионализма.

4.3.3. Получение информации от сотрудников организации

Не углубляясь в аспекты этого способа противодействия угрозам от персонала, отметим, что использование службой ИБ организации информации от персонала организации для выявления потенциальных и фактических злоумышленников может быть весьма эффективным методом защиты. При этом большое значение имеет обеспечение анонимности обращений сотрудников.

Впрочем, массовое и неосторожное использование анонимной информации может иметь потенциальные негативные аспекты в форме нарушения атмосферы доверия в коллективе, а также принятия службой ИБ неверных решений из-за ложных сообщений.

Более подробно с данной категорией защитных мер можно ознакомиться, например, в книге А. И. Доронина «Бизнес-разведка» [54].

Выше была отмечена важность создания культуры безопасности в организации, элементом которой является формирование у сотрудников установки на выявление различных угроз для организации и на информирование ответственных лиц организации о таких угрозах.

4.3.4. Организационные аспекты

Комплексный характер проблемы и организации противодействия демонстрирует, что

различные функции противодействия должны быть возложены на различные подразделения организации, компетентные в соответствующих областях, – кадровую службу, юридический отдел, топ-менеджмент и линейных менеджеров, службу информационной безопасности, подразделение экономической безопасности. Только комплексный подход позволит обеспечить максимальный контроль за проблемами ИБ, связанными с персоналом.

Общая координация противодействия угрозам ИБ от персонала может быть возложена на службу безопасности организации, как непосредственно ответственную за противодействие различным умышленным угрозам, или на одного из топ-менеджеров организации, курирующего вопросы внутренней безопасности.

4.3.5. Скрытность противодействия

Можно быть уверенным, что внутренний злоумышленник, хорошо информированный о всех возможностях системы защиты, включая слабости и ограничения, будет искать и наверняка найдет способ обхода этой защиты, использовав при необходимости свои полномочия или введя в заблуждение коллег.

Хорошей практикой необходимо считать поддержание информационной неопределенности у персонала относительно характеристик по крайней мере части применяемых защитных мер. Такая неопределенность будет производить несколько эффектов:

– недостаточно информированный злоумышленник будет остановлен с большей вероятностью;

– недостаток информации будет производить сдерживающее воздействие на неинформированного злоумышленника даже тогда, когда фактически применяемые защитные меры обладают слабостями.

Скрытность очень важна как в отношении обнаруживающих мер, так и в отношении некоторых превентивных мер. Она обеспечивает эффективность этих мер, поскольку неинформированный злоумышленник будет действовать без учета данных мер и будет обнаружен.

Следующим этапом эволюции защитных мер является сознательное введение потенциальных злоумышленников в заблуждение, в частности:

– применение ложных защитных мер (они неотличимы от реальных, однако не функционируют, их главное преимущество заключается в дешевизне при очевидном сдерживающем воздействии);

– создание ложных информационных активов для отвлечения внимания злоумышленника от реальных ценностей организации; объекты-ловушки, маркированные информационные объекты и другие средства позволяют выявить не связанный с должностными обязанностями интерес к определенным объектам, документы «не на своем месте» и другие важные факты.

4.3.6. Управление системой ролей

Цель любой организации достигается в результате скоординированных действий участников (сотрудников) этой организации. При этом сами действия обычно заранее планируются и распределяются между сотрудниками организации в виде отдельных задач (функций, обязанностей). Состав задач и их распределение между сотрудниками могут оставаться неизменными на протяжении длительного времени, а могут изменяться в силу различных причин, таких как:

– изменение целей организации;

– оптимизация деятельности организации, например, с целью снижение издержек или уменьшения операционных рисков;

– адаптация деятельности организации под новые условия внешней среды, например, под потребности клиентов или под требования регулирующих органов;

– адаптация деятельности организации под новые условия внутренней среды, например, в связи с изменением состава сотрудников организации или в связи с внедрением специализированных средств автоматизации.

Распределение задач между сотрудниками предполагает предоставление каждому из них соответствующего объема ресурсов, необходимых для выполнения задач. Предоставленные организацией сотруднику ограниченные права, разрешения на использование определенных ресурсов организации составляют его полномочия.

При этом результативное и эффективное выполнение сотрудником его задач требует, чтобы предоставленные ему полномочия соответствовали, были достаточны для выполнения этих задач. Недостаточный объем полномочий у сотрудника организации ставит под угрозу достижение намеченных целей, что для организации недопустимо. В этой связи в большинстве компаний можно наблюдать ситуацию, когда ***объем предоставленных сотруднику полномочий несколько превышает объем, достаточный для выполнения его задач.*** Отметим, что такая ситуация в большинстве случаев неизбежна, поскольку:

– всегда существует неопределенность относительно того, какие действия потребуются от сотрудника для выполнения его задачи, и относительно того, сколько в точности ресурсов будет необходимо для выполнения задачи;

– точная регламентация всех полномочий и их применения, а тем более исполнение регламентов весьма трудоемки для большинства организации;

– наиболее значительными полномочиями обладает менеджмент организации, который по ряду причин, в том числе объективных, не склонен ограничивать собственные полномочия.

Как следует из приведенного выше определения угроз ИБ от персонала, полномочия сотрудника в значительной мере определяют исходящие от него риски ИБ для организации. В примитивной форме эту зависимость можно описать так: чем больше объем полномочий, предоставленных сотруднику, тем больше исходящий от него риск ИБ.

В простейшем случае опасность совокупности полномочий, назначенных сотруднику, может быть охарактеризована объемом потенциальных негативных последствий для организации от возможного использования этих полномочий против интересов организации. В более сложных случаях необходимо учитывать, что нападения инсайдеров различных профессий (наделенных различными типами полномочий) существенно отличаются друг от друга, в том числе по характеру и объему негативных последствий для организации [55].

Задача сравнения опасности различных полномочий (например, бухгалтера, системного администратора и начальника производственного участка), по-видимому, не может быть решена иначе, как путем обобщения мнений компетентных лиц, экспертов. Каждая организация вправе выбрать способ сравнения «под себя», заложив в него собственный опыт и представления об угрозах ИБ от персонала.

Следует отметить, что распределение полномочий между сотрудниками обычно неравномерно (в смысле опасности) в силу различных причин – характера решаемых сотрудниками задач, их навыков, возможной оперативной необходимости или даже в результате случайного стечения обстоятельств. Некоторые сотрудники получают на время или постоянно вместе с обязанностями значительный объем полномочий, существенно превосходящий (по опасности) полномочия других сотрудников организации. Такую ситуацию – наличие в организации сотрудника, нецелевое использование полномочий которого может вызвать неприемлемые для организации негативные последствия, – будем называть ***концентрацией*** полномочий. Понятно, что для организации желательно, чтобы концентрация полномочий была исключена или по крайней мере количество «опасных» в этом смысле сотрудников было минимальным. В случаях, когда исключить концентрацию

полномочий невозможно, целесообразно воздействие организации на другие факторы риска из числа перечисленных в подразделе 4.2.3, например, на факторы, связанные с контролируемостью соответствующих полномочий, или на факторы, связанные с мотивационной сферой соответствующих сотрудников.

Очевидный способ уменьшения связанного с концентрацией полномочий риска ИБ состоит в целенаправленном контроле над распределением полномочий в организации. Будем называть деятельность, реализующую такой контроль с целью предотвращения угроз ИБ от персонала, ***управлением системой ролей.***

Можно выделить следующие способы, обычно используемые для описания распределения полномочий между сотрудниками организации:

– слабо формализованное описание, основанное на устных договоренностях или документальных соглашениях произвольной формы;

– систематизированное описание отношений с помощью организационно-функциональных схем, положений о подразделениях и должностных инструкций;

– описание процессов деятельности организации и соответствующей системы ролей сотрудников.

Перечисленные способы не способны полностью функционально заменить друг друга, и во многих организациях такие способы применяются совместно. Кроме того, все они обычно увязывают распределяемые полномочия с задачами (функциями), для решения которых такие полномочия необходимы.

Слабо формализованное описание распределения полномочий обычно характерно для небольших организаций, деятельность которых требует высокой гибкости и (или) в которых руководитель имеет возможность и считает необходимым непосредственно отдавать распоряжения и контролировать деятельность всех сотрудников.

Организационно-функциональная схема описывает общие контуры структуры организации и связывает структурные элементы организации (подразделения и должности) с различными задачами (или видами деятельности организации). Организационно-функциональная схема обычно используется в качестве справочного материала, высокоуровневого представления, которое позволяет сразу увидеть в общих чертах устройство организации (организационную структуру, распределения между подразделениями задач и полномочий). Обратная сторона такова, что формат организационно-функциональной схемы просто не позволяет охватить многие важные детали. Отметим, например, что при чтении схемы, где на одном горизонтальном уровне показаны несколько субъектов, может сложиться ложное впечатление о сопоставимости их задач и полномочий.

Основными правовыми актами, описывающими систему распределения полномочий, в большинстве организаций являются положения о подразделениях и должностные инструкции. В положении о подразделении организации обычно определяются:

– место подразделения в организационной структуре;
– цели и задачи подразделения;
– полномочия подразделения;
– структура и численность подразделения;
– ответственность подразделения.

В должностной инструкции обычно определяются:

– название должности и соответствующего подразделения;
– перечень функций сотрудника;
– обязанности и полномочия (права);
– принципы взаимоотношения с руководством, коллегами и подчиненными.

Наиболее часто в положениях о подразделениях и должностных инструкциях встречаются следующие недостатки:

– отсутствие четких формулировок, что ведет к пересечению функций различных субъектов в организации (сотрудников и подразделений);

– потеря документом актуальности, соответствия реальным отношениям и деятельности;

– несоответствие функций, полномочий и ответственности;

– неполнота перечня функций;

– ориентация функций и полномочий на текущую деятельность при игнорировании функций, связанных с развитием и совершенствованием;

– слабая формализация «горизонтального» взаимодействия между сотрудниками и подразделениями. Реальная эффективность такого взаимодействия часто зависит от того, сложились или нет личные отношения между руководителями соответствующих подразделений.

Выделение роли, как альтернативного должности способа объединения полномочий и обязанностей сотрудника изначально возникло в связи с потребностью менеджмента в снижении сложности различных задач организационного проектирования. Более конкретно: рассмотрение (при проектировании, исследовании или реинжиниринге) некоторого вида деятельности организации, которое осуществлялось отдельно от других видов деятельности той же организации, требовало отдельного рассмотрения участников этого вида деятельности. Любой сотрудник организации при решении такой задачи был интересен только с точки зрения его участия в конкретной рассматриваемой деятельности. Иначе говоря, была интересна его ***роль.*** Если учесть, что почти любой сотрудник участвует в нескольких видах деятельности организации, то понятно, что такой сотрудник выполняет сразу несколько ролей.

Таким образом, роль может быть выделена и необходима только в связи с необходимостью выделения и отдельного рассмотрения определенного вида деятельности в организации. Роль представляет собой более мелкий (по сравнению с должностью) элемент распределения обязанностей и полномочий между сотрудниками.

Правильно реализованное ролевое описание полномочий лишено некоторых недостатков должностной инструкции:

– ролевое описание более гибкое, поскольку в случае изменений требуются меньшие усилия для реорганизации системы обязанностей и полномочий сотрудников;

– система ролей с меньшей вероятностью (чем система должностных инструкций) будет содержать всевозможные пересечения, противоречия и неточности, поскольку она формируется для отдельных видов деятельности, где такие недостатки проще отследить и исключить;

– ролевая система дает больше возможностей точно описать горизонтальные взаимодействия между сотрудниками.

С точки зрения минимизации концентрации полномочий для предотвращения угроз ИБ от персонала ролевое описание полномочий можно считать наиболее подходящим, поскольку оно:

– дает более детальное описание полномочий, чем другие способы;

– более четко, чем другие способы, отражает соответствие полномочий и ситуаций, в которых разрешено их применение;

– позволяет быстро формировать и оценивать различные сочетания полномочий сотрудников.

Описанная выше задача распределения полномочий с целью минимизации их концентрации наиболее эффективно решается посредством формирования и структуризации

системы ролей в организации.

При распределении полномочий на основе системы ролей концентрация полномочий может возникнуть в результате двух ситуаций (см. рис. 68):

– недопустимого (опасного) совмещения функций в одной роли;

– недопустимого (опасного) совмещения функций, которые относятся к разным ролям, но роли назначены одному исполнителю.

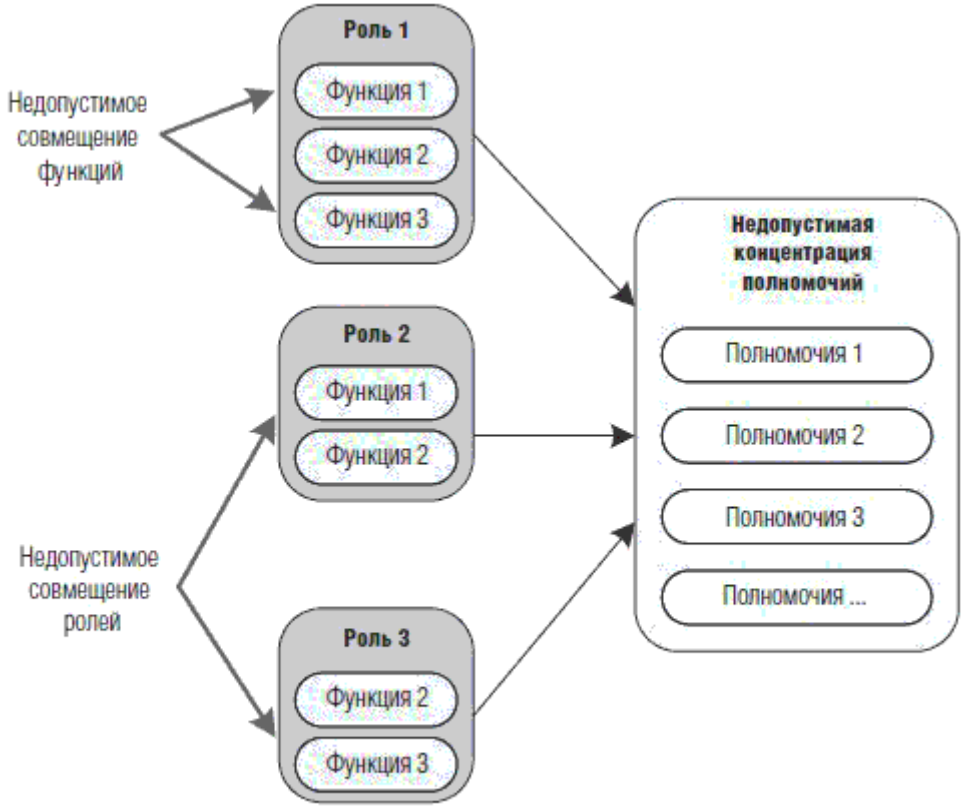


Рис. 68. Возможные причины концентрации полномочий у одного сотрудника

Состав функций, совмещение которых следует считать недопустимой концентрацией полномочий, должен быть определен организацией, исходя из собственных потребностей и практики. В качестве примера требований к формированию ролей и их назначению можно привести положения стандарта Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [26] и положения Банка России № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» [56]. Например, в соответствии с пунктом 7.2.3 стандарта Банка России СТО БР ИББС-1.0-2008 с целью снижения рисков нарушения ИБ не рекомендуется совмещение следующих ролей одним сотрудником:

– разработки и сопровождения системы/ПО;

– разработки и эксплуатации системы/ПО;

– сопровождения и эксплуатации системы/ПО;

– администратора системы и администратора ИБ;

– выполнения операций в системе и контроля их выполнения.

В соответствии с положением Банка России № 242-П не рекомендуется назначение одному и тому же подразделению и (или) служащему функций, связанных с:

– совершением банковских операций и других сделок и осуществлением их регистрации и (или) отражением в учете;

– выдачей санкций на выплату денежных средств и осуществлением (совершением) их фактической выплаты;

– проведением операций по счетам клиентов организации и счетам, отражающим

собственную финансово-хозяйственную деятельность организации;

– предоставлением консультационных и информационных услуг клиентам организации и совершением операции с теми же клиентами;

– оценкой достоверности и полноты документов, представляемых при выдаче кредита, и осуществлением мониторинга финансового состояния заемщика;

– совершением действий в любых других областях, где может возникнуть конфликт интересов.

В общем виде деятельность по управлению системой ролей в организации (в целях уменьшения рисков ИБ) состоит в последовательном решении следующих задач (см. рис. 69):

– идентификация системы ролей;

– оценка системы ролей;

– оптимизация системы ролей.

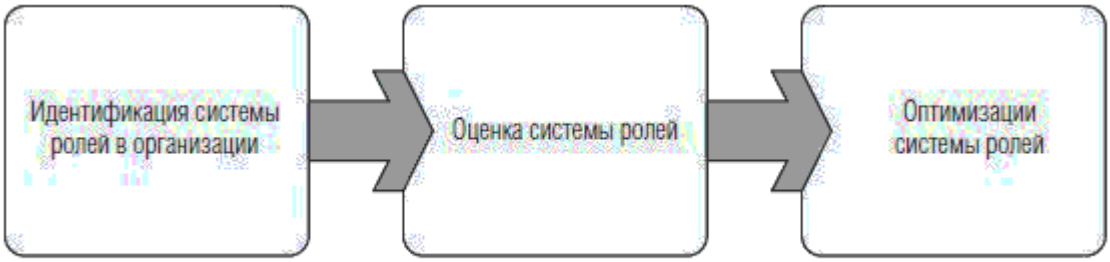


Рис. 69. Основные задачи управления системой ролей в организации

При решении перечисленных задач удобно использовать матричные модели распределения полномочий. Один из возможных форматов матричной модели представлен на рис. 70.

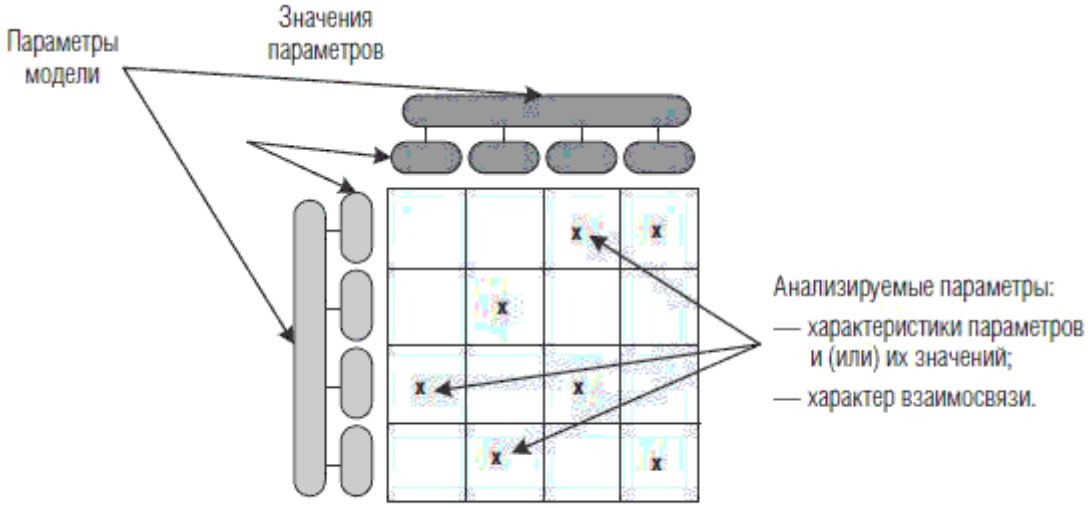


Рис. 70. Обобщенное представление матричной модели

Из рис. 70 видно, что для построения матричной модели должен быть определен состав параметров модели и их значений, а также определен состав параметров отражаемых на пересечении строк и столбцов матричной модели (анализируемые параметры). При этом состав указанных параметров зависит от назначения матричной модели и от состава решаемых задач.

На первом этапе, при идентификации системы ролей, за основу для построения матричной модели целесообразно принимать систему распределения задач и полномочий, описанную действующими в организации должностными инструкциями, положениями о структурных подразделениях и другими документами (регламентами, распоряжениями о предоставлении полномочий и др.). Возможный вид матричной модели показан на рис. 71.

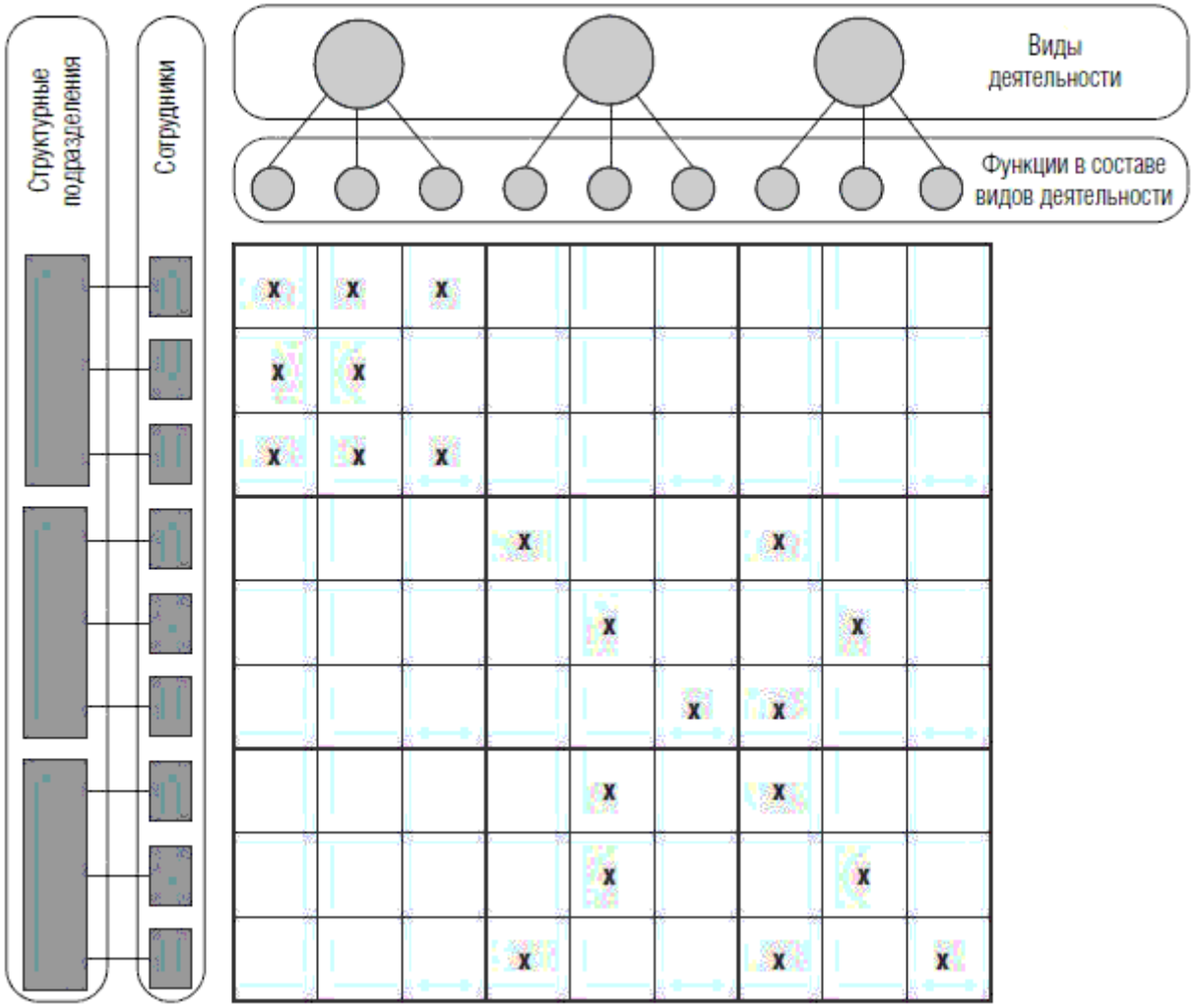


Рис. 71. Матричная модель для идентификации ролей в организации

Для формирования такой матричной модели необходимо наличие хотя бы простой модели деятельности организации, в которой выделены собственно виды деятельности организации, например в виде процессов (идеи процессного представления деятельности кратко рассмотрены в главе 2), и выделены функции – структурные элементы видов деятельности (для процессного формата описания деятельности – процедуры).

Необходимые для формирования матричной модели элементы организационно-штатной структуры и связи между ними могут быть восстановлены по нормативным и организационно-распорядительным документам организации. Целесообразно также проведение опроса некоторых сотрудников организации с целью проверки актуальности восстановленных данных и их дополнения не отраженными документально отношениями.

Следующий шаг идентификации системы ролей состоит в отражении в матричной модели участия сотрудников в выполнении функций. Если сотрудник организации участвует в выполнении некоторой функции, то в соответствующей ячейке матрицы делается отметка, например «х». Состав допустимых отметок должен быть установлен, например, так:

– В – выполняет;
– К – контролирует;
– О – отвечает;
– И – информируется о результатах;
– С – согласовывает решения и (или) консультирует.

На основании заполненной матрицы осуществляется выделение ролей в соответствии с

некоторыми заранее установленными правилами, например:

– роли идентифицируются отдельно для каждого вида деятельности, т. е. не должно быть ролей, входящих одновременно в более чем один вид деятельности;

– если за разными сотрудниками закреплена одна и та же группа функций в рамках одного вида деятельности, то такая группа функций идентифицируется как роль;

– если за одним или несколькими сотрудниками организации закреплена группа функций, отличающаяся от функций других сотрудников в рамках того же вида деятельности, то указанная группа функций идентифицируется как роль.

В результате описанной деятельности будет сформирован перечень ролей, а содержание ролей (обязанности и полномочия) может быть описано в терминах соответствующих видов деятельности организации.

Полученный результат не только позволит перейти к следующему этапу – оценке системы ролей с точки зрения ИБ, но и даст возможность руководству организации по-новому взглянуть на существующее в организации и закрепленное в ее нормативной базе распределение обязанностей и полномочий.

Оценка ролей в организации фактически заключается в выявлении ситуаций концентрации полномочий двух типов:

– недопустимого (опасного) совмещения функций в одной роли;

– недопустимого (опасного) совмещения функций, которые относятся к разным ролям, но роли назначены одному исполнителю.

Эти две задачи решаются сходным способом. Поэтому деятельность по оценке ролей покажем на примере решения первой задачи.

Для осуществления оценки системы ролей с целью выявления в них недопустимого совмещения функций используется матричная модель распределения функций между ролями, пример которой приведен на рис. 72.

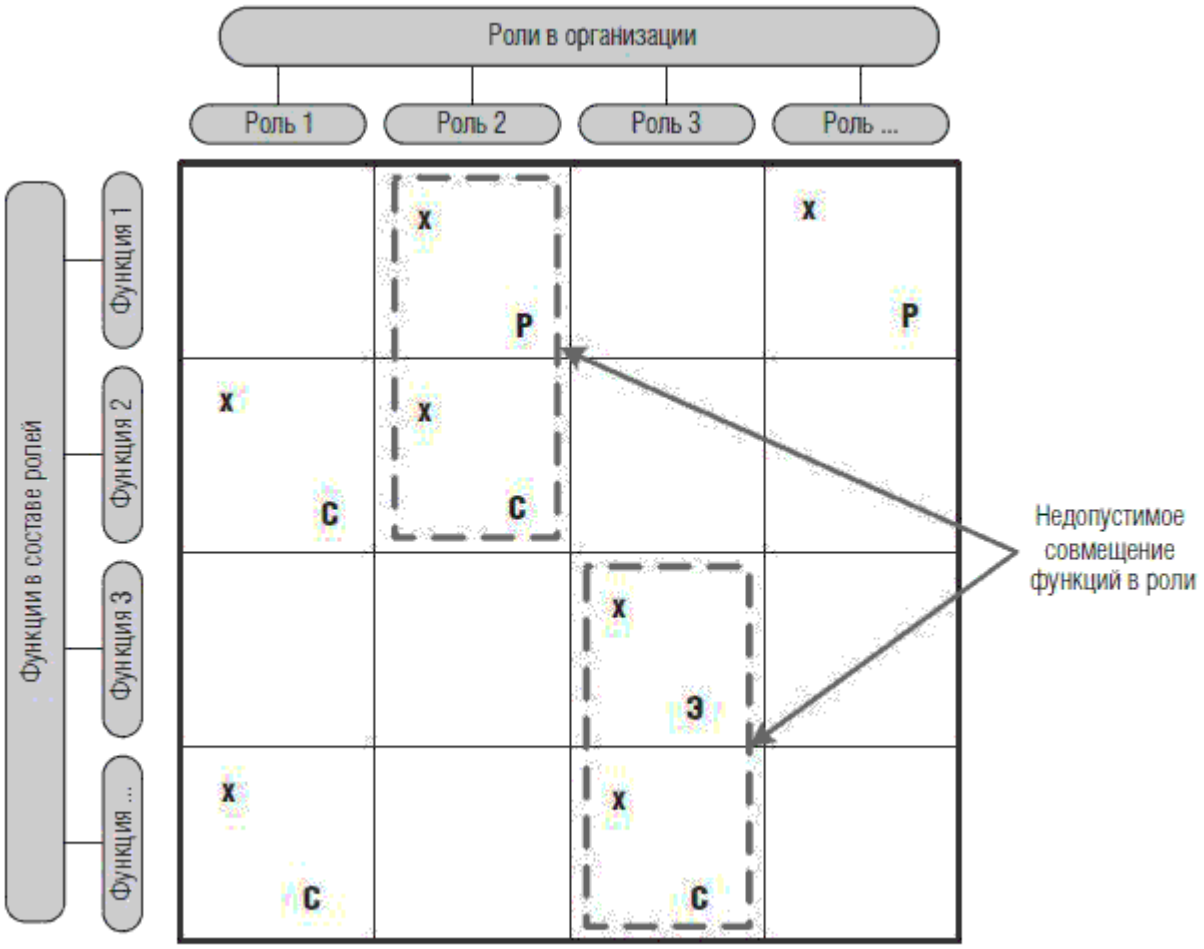


Рис. 72. Матричная модель распределения функций между ролями

Такая матричная модель распределения функций между ролями отражает состав функций закрепленных за ними. Формирование матричной модели распределения функций между ролями осуществляется на основании перечня ролей организации, который был сформирован на предыдущем этапе – идентификации ролей.

Анализ матричной модели распределения функций между ролями выполняется с целью выявления недопустимого совмещения функций в ролях, а его результатом является перечень ролей, в которых обнаружено недопустимое совмещение функций, и перечень собственно пар совмещенных функций.

После того как определена принадлежность функции, в матричной модели рядом с отметкой «х» ставится отметка в виде условного обозначения соответствующей функций недопустимой для совмещения, как представлено на рис. 72. Для удобства заполнения матричной модели и ее дальнейшего анализа рекомендуется использовать различные условные обозначения для групп функций недопустимых для совмещения, например:

– функции, связанные с разработкой программных средств, – Р;
– функции, связанные с сопровождением программных средств, – С;
– функции, связанные с эксплуатацией программных средств, – Э.

Недопустимым для совмещения функции могут быть обнаружены поиском в столбцах матрицы (выделено пунктирным контуром на рис. 72).

Выявление недопустимого совмещения ролей при назначении одному сотруднику выполняется аналогичным образом. В ходе деятельности по оценке ролей организации в качестве рабочих материалов формируются две матричные модели (модель распределения функций между ролями и модель распределения ролей между сотрудниками), а также следующие перечни:

– перечень ролей, в которых выявлено недопустимое совмещение функций;

– перечень сотрудников организации, которым назначены недопустимые для совмещения роли.

Оптимизация системы ролей организации проводится путем внесения изменений по двум направлениям:

– перераспределение функций между ролями с целью устранения недопустимого совмещения функций в отдельных ролях;

– перераспределение ролей между сотрудниками организации с целью устранения недопустимого совмещения ролей сотрудниками.

Оптимизация системы ролей проводится на основе результатов оценки системы ролей в организации.

Перераспределение функций между ролями может быть выполнено путем применения необходимых сочетаний следующих операций:

– удаление функции из роли;

– перемещение функции между ролями;

– создание новых ролей для перемещения в них функции.

При перераспределении функций между ролями целесообразно использовать матричные модели, полученные в ходе оценке системы ролей (см. пример на рис. 73).

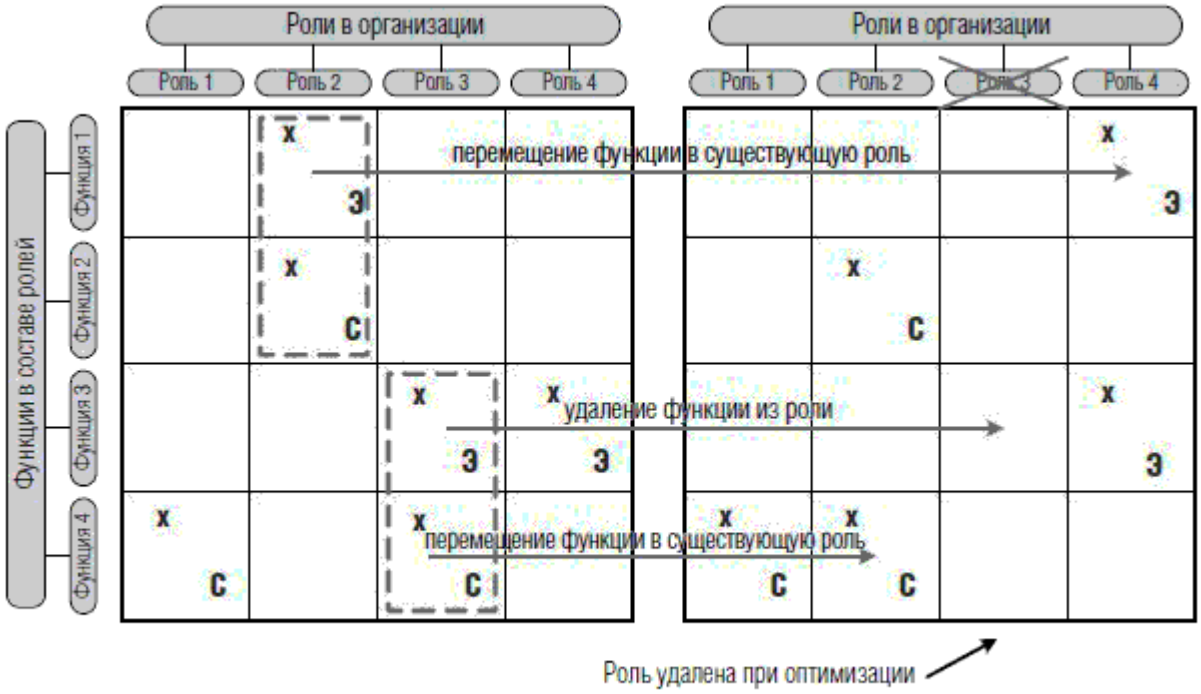


Рис. 73. Пример перераспределения функций ролей

Для перераспределения ролей между сотрудниками организации (переназначение ролей) с целью устранения недопустимого совмещения ролей сотрудниками организации могут быть использованы сочетания аналогичных приемов:

– сотрудник может быть освобожден от исполнения одной из ранее назначенных ему ролей;

– сотруднику может быть назначена некоторая роль в дополнение к уже выполняемым им ролям;

– может потребоваться прием на работу нового сотрудника и назначение ему роли, которая не может быть назначена имеющимся сотрудникам из-за концентрации полномочий.

По результатам перераспределения функций внутри ролей и (или) перераспределения ролей между сотрудниками организации формируются обновленные матричные модели. На их основе может быть актуализирована правовая база организации (ролевые инструкции, регламенты, должностные инструкции, описания видов деятельности) и изменена собственно технология деятельности.

Отметим, что при различных изменениях в организации, таких как изменение состава видов деятельности или увольнение/прием на работу сотрудников, система ролей должна переоцениваться с точки зрения концентрации полномочий, а по результатам оценки должны приниматься меры по оптимизации системы ролей.

Отметим, что возможными препятствиями для деятельности по управлению системой ролями могут стать:

– невозможность собрать ту или иную информацию, необходимую для управления системой ролей (в частности, невозможность сформировать достаточно детальное описание видов деятельности, невозможность сформировать достаточно детальное описание распределения полномочий, невозможность сформировать суждения относительно опасности различных сочетаний полномочий);

– противоречие между предложениями информационной безопасности относительно необходимости перераспределения ролей и представлениями бизнеса относительно эффективной организации труда;

– инерционность организации при осуществлении оптимизации системы ролей, включая следующие:

– сопротивление персонала (в качестве мотивов вероятны борьба за сохранение концентрации полномочий, борьба за сохранение бесконтрольности, а также сопротивление изменениям как потенциальной опасности);

– необходимость модернизации технологической среды, например используемых прикладных программных средств;

– негативное влияние изменений на эффективность деятельности организации, поскольку отдельные функции перейдут к новому, возможно, недостаточно опытному в этой сфере исполнителю, в связи с чем качество их выполнения может пострадать. Новому исполнителю потребуется время на то, чтобы установить контакты, необходимые для выполнения функций.

Управление системой ролей наиболее целесообразно применять в основном в тех видах деятельности организации, где рабочий процесс является неизменным в течение достаточно продолжительного времени, что позволяет однократно уделить время грамотному выделению и распределению ролей и пользоваться его результатами продолжительное время.

4.3.7. Программно-технические средства защиты от утечек информации

Как было отмечено выше, одной из серьезных угроз от персонала является угроза утечки служебной информации. Подобные инциденты часто на слуху из-за широкого круга затронутых лиц. Утечки конфиденциальной информации облегчаются существованием многочисленных каналов, доступных почти каждому сотруднику организации и связывающих корпоративные сети организаций с Интернетом (к их числу относятся месседжеры, электронная почта), распространением съемных носителей информации большого объема, легко подключаемых почти к любому компьютеру, а также распространением беспроводных сетей.

В последнее десятилетие быстро сформировался отдельный сегмент рынка соответствующих специализированных защитных мер – систем защиты от утечек, DLP. Данные средства ориентированы на выявление и блокирование ситуаций утечки конфиденциальной информации по каналам связи. Участники рынка активно продвигают

такие средства под флагом «борьбы» с инсайдерами, с внутренними угрозами ИБ. При том что прогресс в развитии подобных технических средств можно оценить только положительно, необходимо помнить, что только комплексный подход (см. выше) позволит решить проблему. Угрозы от персонала не исчерпываются одними лишь утечками, другие угрозы являются не менее опасными и редкими. В то же время фактически происходящие утечки информации не ограничены каналами, контролируемыми посредством защитных мер DLP (чего стоит только устно передаваемая служебная информация), а эффективное применение DLP требует серьезных организационных политик в области классификации информации и в области управления оборотом служебной информации.

Это лишь один из инструментов, который поодиночке не позволит решить задачу в целом. Кроме того, такие средства требуют тщательной настройки с периодической актуализацией настроек.

4.3.8. Расследование инцидентов

Инцидент, в котором замешан сотрудник организации, для большинства организаций – чрезвычайное происшествие. Поэтому способ организации расследования сильно зависит от сложившейся корпоративной культуры организации. Но можно уверенно сказать: важно продумать заранее и зафиксировать организационные политики по расследованию таких инцидентов, включая состав и основные роли участников расследования, условия предоставления и объем чрезвычайных полномочий по получению информации при расследовании, возможные меры в отношении сотрудников, причастных к инциденту.

Расследование выявленного инцидента – информационный процесс, один из этапов реагирования на инцидент. Сбор и документирование информации об инциденте целесообразно начинать уже с момента его обнаружения, а желательно еще раньше – при выявлении предвестников инцидента.

Целями расследования обычно являются:

– восстановление хода инцидента;

– выявление участников инцидента (в том числе из числа сотрудников) и их ролей в ходе инцидента;

– сбор свидетельств и предварительная оценка степени вины сотрудников в инциденте;

– сбор юридически значимых материалов, пригодных для инициирования процедур, обеспечивающих привлечение виновных лиц к ответственности;

– выявление причин и условий инцидента, включая недостатки системы защиты организации, формирование предложений по совершенствованию системы защиты;

– сбор свидетельств и оценка негативных последствий инцидента.

Для успешного расследования крайне важно наличие механизмов регистрации действий сотрудников в расследуемой сфере деятельности.

Отметим, что определение вины сотрудника может быть весьма сложной задачей при проведении внутреннего расследования, поскольку обосновывающие умысел факты часто отсутствуют. К подобным фактам можно отнести:

– неоднократность инцидентов, связанных с сотрудником;

– подтвержденная заинтересованность сотрудника в последствиях инцидента;

– попытки сокрытия сотрудником следов своих действий, связанных с инцидентом;

– наличие следов заблаговременной подготовки сотрудника к инциденту;

– высказывания сотрудника до инцидента, свидетельствующие о его мотивах и намерениях.

Обращение к правоохранительным органам может потребоваться в случае, когда есть основания в умышленном характере инцидента; есть основания для уверенности во внешней поддержке злоумышленника, причинен или мог быть причинен существенный ущерб

организации или третьим лицам.

Техническая сторона действий внутреннего злоумышленника зачастую настолько выражена в инцидентах ИБ, что для проведения внутреннего расследования может потребоваться использование специализированных программных средств, позволяющих получить необходимые свидетельства с устройств хранения и обработки информации, принадлежащих организации.

Отметим, что любое внутреннее расследование, пусть и без привлечения правоохранительных органов, – всегда стресс для коллектива. Среди возможных негативных последствий для организации: наказание невиновных, напряженность в коллективе, отвлечение сотрудников от работы и др.

4.3.9. Раскрытие информации об инцидентах

Вопросы раскрытия информации о различных инцидентах внутри и вне организации являются весьма значимыми для большинства организаций. При этом вполне обоснованы опасения менеджмента большинства организаций относительно возможных негативных последствий от раскрытия информации.

Такие негативные последствия могут наступить в форме реакции рынка – снижения капитализации компании, реакции акционеров по отношению к менеджменту организации, реакции клиентов и партнеров в форме изменения решений по совместной работе, реакции регуляторов в форме повышения планки различных требований (например, требований по резервированию капитала или обеспечения защиты от различных угроз) и проведения внеплановых проверок, а также конкурентов в форме осуществления черного пиара. Поток негатива о компании может сильно повлиять на ее имидж на рынке и на выполнение бизнес-планов даже в условиях небольших прямых потерь от собственно инцидентов.

Между тем раскрытие информации может оказаться необходимым организации для применения санкций в отношении злоумышленника и его сообщников, организации возврата материальных и других активов, обеспечения осведомленности персонала, выполнения законных требований регулирующих органов и собственников компании, а также выполнения соглашений с партнерами и клиентами.

Кроме того, позиция полного сокрытия информации об инцидентах может оказаться неприемлемой, поскольку информация так или иначе (очень вероятно, что в искаженной форме) все равно будет просачиваться к ее потенциальным потребителям. Сплетни и слухи, оставаясь без официальных комментариев организации, будут формировать ее имидж как скрытного и потенциально ненадежного партнера, риски работы с которым неприемлемо высоки. Естественно, что происшествия различного рода случаются в любой организации, и утверждения о полном их отсутствии вызовут улыбку у любого специалиста или руководителя.

Приведенные аргументы убеждают, что организациям необходимо тщательно прорабатывать вопросы информационной политики в части дозирования выдаваемой во внешний мир информации по инцидентам, определения способа подачи такой информации, выбора момента подачи информации, определения состава первых ретрансляторов информации (СМИ, ресурсов Интернет и др.), а также по выбору ответственных за внутреннюю и внешнюю информационную политику сотрудников компании.

Хорошей практикой является индивидуальное информирование собственников, партнеров и клиентов по крупным инцидентам, затрагивающим их интересы.

Приложение 1
Архитектура стандартов защиты информации и обеспечения информационной безопасности

Общие сведения

Стандарты по защите информации и обеспечения информационной безопасности, используемые в российских организациях, имеют различное происхождение, различия и общности в объектах и аспектах стандартизации.

Если рассматривать чисто российские документы, то такие стандарты носят, как правило, форму требований технического характера преимущественно к компонентам технологической среды или справочного назначения, например ГОСТ Р 51275 («Факторы, воздействующие на информацию. Общие положения»). В редких случаях российские национальные стандарты являются основанием для соответствующих систем сертификации, такие как стандарты на алгоритмы криптографических преобразований (ГОСТ Р 34.10, ГОСТ Р 34.11, ГОСТ 28147).

Если термин «защита информации» («техническая защита информации») исторически используется в РФ и нормативно закреплен руководящими документами от 1992 г. Гостехкомиссии при Президенте РФ (Федеральная служба по техническому и экспортному контролю), то термин «информационная безопасность» (information security) чаще ассоциируется с положениями зарубежных (гармонизированных в РФ) стандартов. В то же время методологически все эти понятия имеют в основе одну и ту же модель, оформившуюся в середине 1980-х гг. («оранжевая» книга США, аналогичные документы Германии, Великобритании и других стран) и получившую различное развитие на уровне отдельных стран и международном уровне.

Практически до 1990-х гг. устоявшегося однозначного понятийного аппарата для предметной области безопасности в сфере информатики (информации) не существовало. На практике использовали различные термины и их определения, зачастую относящиеся к одному и тому же объекту. В зарубежных документах (стандартах и руководствах) широко использовали такие понятия, как data protection, data safety, data security, information security, IT security и др. В России тех времен все это воспроизводилось полностью и дополнялось национальным колоритом.

Разнообразие подходов и определений в пределах одной и той же области не в последнюю очередь послужило причиной учреждения в рамках международных организаций соответствующих специализированных профессиональных структур, целью деятельности которых являлась выработка единых, согласованных позиций и подходов в сфере безопасности применительно к информатике и информационным технологиям. Например, в 1989 г. в рамках совместного ИСО и МЭК технического комитета 1 (СТК 1) «Информационные технологии» был образован профильный орган (подкомитет) № 27 «Методы и средства обеспечения безопасности». Первоочередной задачей данного подкомитета являлась выработка основополагающих международных стандартов и руководств по базовым технологиям обеспечения безопасности при применении электронных информационных технологий. До этого стандарты, относящиеся к вопросам безопасности, издавались по мере необходимости самыми различными органами (подкомитетами ИСО), например, в рамках стандартизации протоколов и технологий взаимодействия открытых систем, служб и стандартов телекоммуникаций (МККТТ, позже – МСЭ-Т), стандартов Интернет и т. п. Применительно к 27-му подкомитету СТК 1 ИСО/МЭК абсолютно логично началом работ послужили вопросы стандартизации использования криптографических алгоритмов (конек спецов по безопасности информации предшествующих десятилетий) и выработки решений по противодействию внешним и внутренним злоумышленникам (обнаружение вторжений, основные угрозы, уязвимости и контрмеры, методы менеджмента безопасности информационных технологий и т. п.).

Позже (в 1993 г.) в рамках работ 27-го подкомитета СТК 1 ИСО/МЭК было открыто новое направление, преследующее целью формирование основы глобальному рынку средств

безопасности ИТ, в связи с чем была образована соответствующая рабочая группа в структуре подкомитета.

В основу глобального рынка средств безопасности ИТ планировалось заложить подход, нашедший отражение в системе документов, известных как «Общие критерии» (Common criteria). Эта спецификация формально спонсируемая сообществом стран – издательским советом спонсоров технологии, а по сути профильными государственными организациями США. В рамках ИСО данная методология была оформлена серией стандартов, первыми из которых были:

– ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» (в трех частях, свыше 600 страниц спецификаций и требований);

– ИСО/МЭК 18045 «Методология оценки безопасности информационных технологий» (почти 300 страниц требований к действиям оценщика – испытательной лаборатории).

Состояние дел на момент издания первой редакции ИСО/МЭК 15408 в 1999 г. и этапы формирования данного документа иллюстрирует рис. 1.

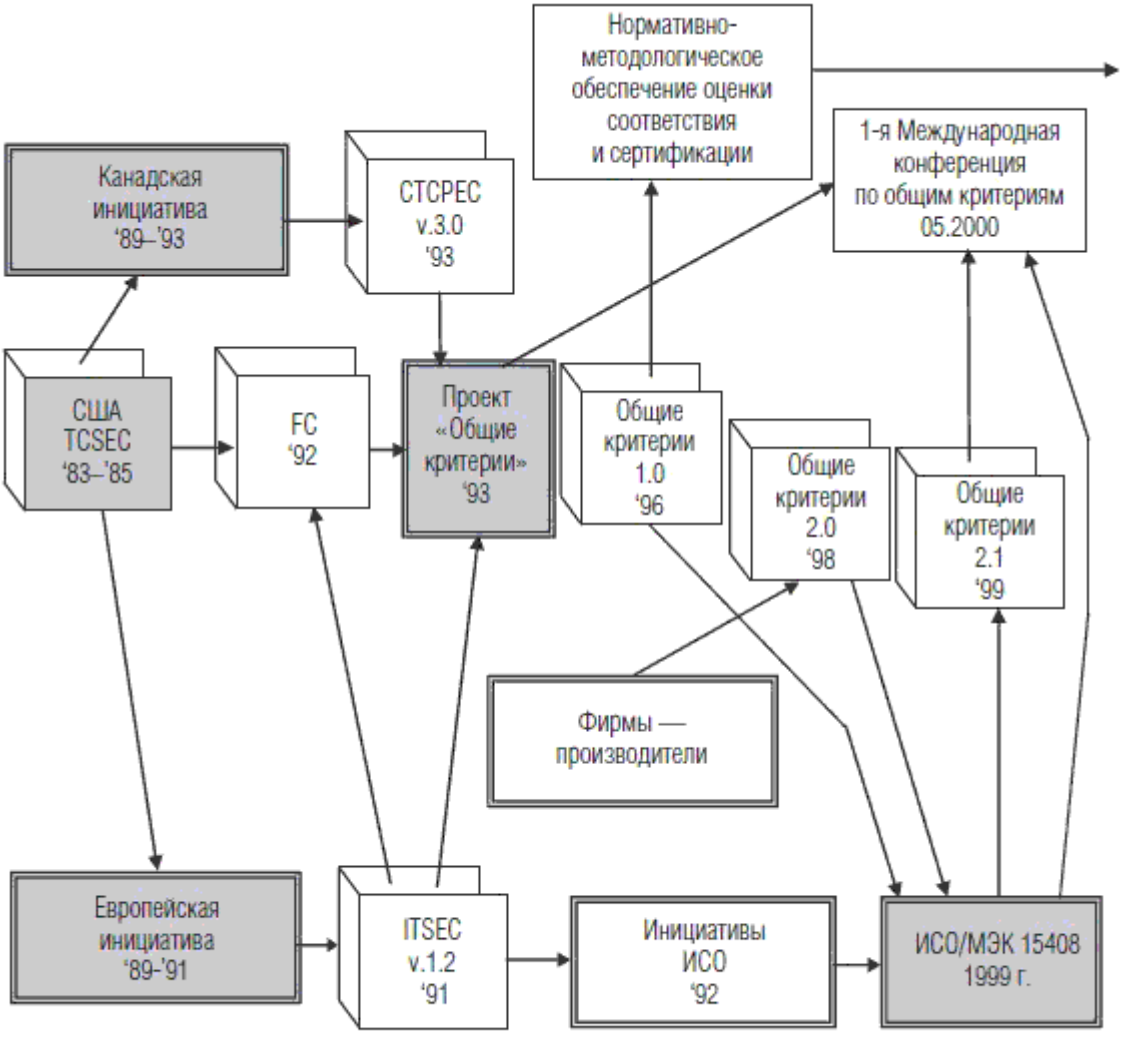


Рис. 1. История развития критериев оценки безопасности информационных технологий

Указанные работы сопровождались выработкой платформы международного признания результатов оценки соответствия и сертификации, поддерживаемые соответствующими межправительственными соглашениями. Инициаторами анонсировались удовлетворяющие различным отраслям решения, что, однако, не всегда подтверждалось практикой.

Например, банковское сообщество в начале 2000-х гг. инициировало проект по выработке рекомендаций банковскому сообществу относительно порядка возможного использования подхода «Общих критериев» в своей деятельности. Данные работы

стартовали под индексом ISO TR 24590 «Banking-protection profiles for the financial industry» («Банковские профили защиты для финансовой отрасли»), но были прекращены на стадии работ в рамках комитета по причине отсутствия перспектив практической целесообразности. «Виной» тому (хотя этот термин не совсем уместен) была невозможность сохранения действия сертификатов по безопасности при реконфигурации сертифицированных изделий ИТ при их использовании в среде организации за пределами той конфигурации, что использовалась при сертификационных испытаниях. Потеря действия сертификата приводила к утрате гарантий органа сертификации (реальных гарантий, поддержанных финансовыми обязательствами), что сводило на нет все преимущества такой сертификации.

Одновременно с этим в России в начале 2000-х гг. параллельно и где-то согласованно, но в различных целях, велись работы по анализу и оценке возможности практического использования подхода «Общих критериев» в рамках развития национальной системы сертификации средств защиты информации и совершенствования систем безопасности в организациях отраслевой принадлежности. Результат был диаметрально противоположным.

По линии развития национальной системы сертификации по требованиям защиты информации подход «Общих критериев» был взят на вооружения (но без присоединения к международному соглашению о признании сертификатов), что виделось как значимый положительный шаг развития существовавших норм и критериев сертификации по требованиям защиты информации.

В части же совершенствования систем безопасности в организациях отраслевой принадлежности (организации банковской системы Российской Федерации) вердикт был аналогичен тому, что был вынесен в рамках международных дискуссий.

Однако подход «Общих критериев» более десятилетия был в центре внимания специалистов по безопасности информации во всех странах мира, рассматривающих его как полезный и прагматичный, потенциально позволяющий решить множество задач обеспечения ИБ организаций. В результате был принят комплекс соответствующих международных стандартов (как уже отмеченных, так и других). Ряд из них был гармонизирован в системе «ГОСТ Р» (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО/МЭК 15446 и др.).

Неудовлетворенность в ожиданиях по результатам исследований и анализ практики использования подхода «Общих критериев», а также все возрастающие потребности в поиске платформы конструктивного взаимодействия безопасности и бизнеса, сместили акценты в срез управленческих задач обеспечения безопасности.

Со временем данные задачи получили свое воплощение в семействе стандартов менеджмента информационной безопасности, требования которых предназначены для охвата всего множество задач обеспечения ИБ организаций. Основные положения и цели стандартов данного семейства были рассмотрены в соответствующих главах настоящего издания. На данной платформе стала возможна выработка качественно новых востребованных решений по унификации и стандартизации аспектов информационной безопасности в прикладных сферах как в стандартизированных процессах информатизации деятельности компаний, так и в специфичных областях бизнеса.

Как итог понимания в принципах организации работ, сбалансированности структуры объектов и аспектов стандартизации сформировалась сбалансированная архитектура системы международных стандартов обеспечения информационной безопасности бизнеса, технологий, целей деятельности. Она дает инструменты разрешения задач обеспечения информационной безопасности организации как на уровне корпоративного управления, так и технического взаимодействия внутри организации и вовне ее, с ее клиентами и партнерами, органами регулирования и надзора.

В Российской Федерации национальные (до 2003 г. – государственные) стандарты по защите информации (информационной безопасности) издавались преимущественно под эгидой Технического комитета № 362 «Защита информации» и Технического комитета № 22 «Информационные технологии» национального органа по стандартизации, где с конца

1990-х гг. активизировались работы по гармонизации международных стандартов. Ряд стандартов прошел совместно. Например, гармонизированный ГОСТ Р ИСО/МЭК 15408 внесен на утверждение Гостехкомиссией России, Техническими комитетами по стандартизации ТК 362Р «Защита информации» и ТК 22 «Информационные технологии». В числе других гармонизированных в России международных стандартов можно отметить ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 17999, ГОСТ Р ИСО/МЭК ТО 18044 и др.

Что касается гармонизации в Российской Федерации международных стандартов по обеспечению информационной безопасности, то их количество пока невелико. Если по линии 27-го подкомитета СТК 1 ИСО/МЭК разработано и развивается свыше 100 международных стандартов (технических отчетов – «предстандартов»), то в Российской системе документов по стандартизации на начало 2010 г. их было не более двух десятков (защита информации и информационная безопасность), включая как исключительно российские, так и гармонизированные международные.

В то же время следует отметить, что наряду с пониманием необходимости изучения зарубежного опыта, а также исходя из потребности решения практических задач процесс гармонизации в России западных стандартов будет неуклонно расширяться.

Рис. 2 иллюстрирует сформировавшуюся на международном уровне обобщенную архитектуру стандартов обеспечения информационной безопасности организации.

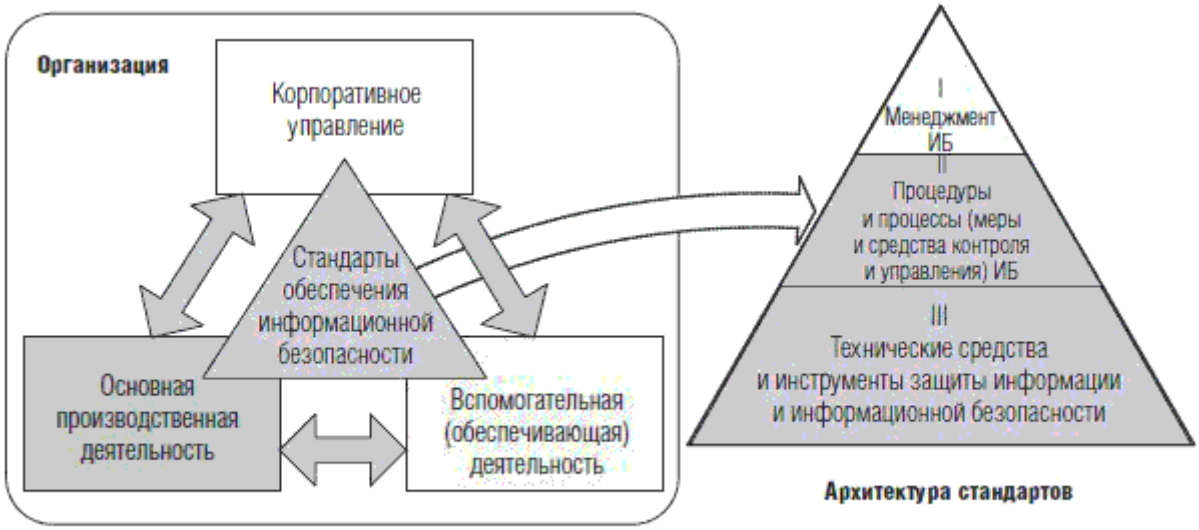


Рис. 2. Обобщенная архитектура стандартов обеспечения информационной безопасности организации

К категории I («Менеджмент ИБ» на рис. 2) можно отнести как стандарты семейства менеджмента ИБ ISO/IEC 270XX (семейство стандартов СМИБ организации), так и комплекс новых стандартов направления Identity management and privacy technologies (менеджмент идентификационными атрибутами и безопасность личности в электронном мире).

Среди российских национальных стандартов к данной категории можно отнести только гармонизированные международные.

К категории II («Процедуры и процессы (меры и средства контроля и управления) ИБ» на рис. 1.2) можно отнести стандарты для следующих объектов и аспектов стандартизации:

– менеджмент инцидентов информационной безопасности;
– безопасность сетей информационных технологий;
– обнаружение вторжений, выбор и поставка систем обнаружения вторжений;
– управление и пользование услугами третьей доверенной стороны;
– восстановление информационных технологий после бедствий и аварий и т. п.

Среди российских национальных стандартов к данной категории можно отнести ГОСТ Р 50922, ГОСТ Р 51275 и др.

К категории III («Технические средства и инструменты защиты информации и информационной безопасности» на рис. 1.2) можно отнести стандарты на алгоритмы

криптографических преобразований, критерии оценки безопасности информационных технологий и т. п. Среди российских национальных стандартов к данной категории можно отнести стандарты требований по защите от несанкционированного доступа к средствам вычислительной техники и автоматизированным системам, гармонизированные международные стандарты критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408), ГОСТ Р ИСО/МЭК 18045), защиты от вредоносного программного обеспечения и т. п. Далее будут приведены сведения по ряду документов национальной и международной системам стандартизации в области защиты информации и обеспечения информационной безопасности. Эти сведения могут быть использованы в справочных целях для решения тех или иных практических задач.

Национальная система стандартизации

Стандарты по защите информации и обеспечению информационной безопасности организации в системе национальных документов по стандартизации регистрируются в основном по следующим кодам международной классификации стандартов:

– 01.040.01 «Общие положения. Терминология. Стандартизация. Документация (Словари)»;

– 35.020 «Информационные технологии (ИТ) в целом»;

– 35.040 «Наборы знаков и кодирование информации».

В число наиболее известных действующих стандартов входят:

– ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

– ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

– ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»;

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

– ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»;

– ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»;

– ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения»;

– ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»;

– ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования»;

– ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения»;

– ГОСТ Р 53109-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности»;

– ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;

– ГОСТ Р 53115-2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа.

Методы и средства»;

– ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»;

– ГОСТ Р ИСО/МЭК ТО 13335 (гармонизированный международный) «Информационная технология. Методы и средства обеспечения безопасности». Включает в себя следующие части: часть 1 «Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»; часть 3 «Методы менеджмента безопасности информационных технологий»; часть 4 «Выбор защитных мер»; часть 5 «Руководство по менеджменту безопасности сети»;

– ГОСТ Р ИСО/ТО 13569-2007 (гармонизированный международный) Финансовые услуги. Рекомендации по информационной безопасности;

– ГОСТ Р ИСО/МЭК 15408 (гармонизированный международный) Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Включает в себя следующие части: Часть 1. Введение и общая модель; Часть 2. Функциональные требования безопасности; Часть 3. Требования доверия к безопасности;

– ГОСТ Р ИСО/МЭК ТО 15446-2008 (гармонизированный международный) «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» ГОСТ Р ИСО/МЭК 17799-2005 (гармонизированный международный) «Информационная технология. Практические правила управления информационной безопасностью»;

– ГОСТ Р ИСО/МЭК ТО 18044-2007 (гармонизированный международный) «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

– ГОСТ Р ИСО/МЭК 18045-2008 (гармонизированный международный) «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»;

– ГОСТ Р ИСО/МЭК 27001-2006 (гармонизированный международный) «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Международная система стандартизации

Международные стандарты по защите информации и обеспечению информационной безопасности организации разрабатываются как в рамках работ 27-го подкомитета СТК 1 ISO/IEC, так и по линии других технических комитетов в плотной кооперации работ с экспертами 27-го подкомитета.

В числе стандартов, принятых в рамках планов работ 27-го подкомитета СТК 1 ISO/IEC, следует отметить такие документ, как:

– ISO/IEC 27000:2009 «Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Обзор и словарь»;

– ISO/IEC 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

– ISO/IEC 27002:2005 «Информационные технологии. Свод правил по управлению защитой информации»;

– ISO/IEC 27003 (проект) «Руководство по реализации СМИБ»;

– ISO/IEC 27004 (проект) «Менеджмент информационной безопасности. Измерения»;

– ISO/IEC 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»;

– ISO/IEC 27006:2007 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем

менеджмента информационной безопасности»;

– ISO/IEC 27007 (проект) «Руководства по аудиту СМИБ»;

– ISO/IEC 27008 (проект) «Руководства для аудиторов по аудиту средств контроля СМИБ»;

– ISO/IEC 27010 (проект) «Менеджмент информационной безопасности для межотраслевого взаимодействия»;

– ISO/IEC 27011:2008 «Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по менеджменту информационной безопасности организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002»;

– ISO/IEC 27013 (проект) «Руководство по совместному использованию стандартов ИСО/МЭК 20000-1 и ИСО/МЭК 27001»;

– ISO/IEC 27014 (проект) «Корпоративное управление информационной безопасностью»;

– ISO/IEC 27015 (проект) «Руководства по менеджменту информационной безопасности для финансового сектора и сектора страхования»;

– ISO TR 13569:2005 «Услуги финансовые. Руководящие указания по обеспечению информационной безопасности» (разработан ИСО ТК 68 «Финансовые услуги»);

– ISO/IEC 7064:2003 «Информационные технологии. Методы и средства обеспечения безопасности. Системы контрольных знаков»;

– ISO/IEC 9796 «Информационные технологии. Методы и средства обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений»;

– ISO/IEC 9797 «Информационные технологии. Методы и средства обеспечения безопасности. Коды аутентификации сообщений (MAC)»;

– ISO/IEC 9798 «Информационные технологии. Методы и средства обеспечения безопасности. Аутентификация объектов»;

– ISO/IEC 10116:2006 «Информационные технологии. Методы и средства обеспечения безопасности. Режимы работы для n-битовых блочных шифров»;

– ISO/IEC 10118 «Информационные технологии. Методы и средства обеспечения безопасности. Хэш-функции»;

– ISO/IEC 11770 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент ключей». Включает в себя следующие части: часть 1 «Структура»; часть 2 «Механизмы, использующие симметричные методы»; часть 3 «Механизмы, использующие асимметричные методы»; часть 4 «Механизмы, основанные на нестойких секретах»; часть 5 «Менеджмент групповых ключей»;

– ISO/IEC 13888 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение авторства»;

– ISO/IEC 14888 «Информационные технологии. Методы и средства обеспечения безопасности. Цифровые подписи с приложением»;

– ISO/IEC 15946 «Информационные технологии. Методы и средства обеспечения безопасности. Криптографические методы на основе эллиптических кривых»;

– ISO/IEC 18014 «Информационная технология. Методы и средства обеспечения безопасности. Услуги по созданию метки даты/времени»;

– ISO/IEC 18031:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Произвольное генерирование битов»;

– ISO/IEC 18032:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Поколение простых чисел»;

– ISO/IEC 18033 «Информационные технологии. Методы и средства обеспечения безопасности. Алгоритмы шифрования»;

– ISO/IEC 19772:2009 «Информационные технологии. Методы и средства обеспечения безопасности. Установленные криптографические методы»;

– ISO/IEC 29150 (проект) «Информационные технологии. Методы и средства обеспечения безопасности. Шифрование подписи»;

– ISO/IEC 29192 (проект) «Информационные технологии. Методы и средства обеспечения безопасности. Облегченная криптография»;

– ISO/IEC 15292:2001 «Информационные технологии. Методы и средства обеспечения безопасности. Процедуры регистрации профилей защиты»;

– ISO/IEC 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ». Включает в себя следующие части: часть 1 «Введение и общая модель»; часть 2 «Функциональные требования безопасности»; часть 3 «Требования к обеспечению защиты»;

– ISO/IEC TR 15443-1:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Структура обеспечения доверия в безопасности IT». Включает в себя следующие части: часть 1 «Обзор и структура»; часть 2 «Методы обеспечения доверия»; часть 3 «Анализ методов обеспечения доверия»;

– ISO/IEC TR 15446:2009 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»;

– ISO/IEC 18045:2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности ИТ»;

– ISO/IEC 19790:2006 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к защите применительно к криптографическим модулям»;

– ISO/IEC TR 19791:2006 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности эксплуатирующихся систем»;

– ISO/IEC 19792:2009 «Информационные технологии. Методы и средства обеспечения безопасности. Оценка безопасности биометрии»;

– ISO/IEC 21827:2008 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса»;

– ISO/IEC 24759:2008 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к тестированию криптографических модулей»;

– ISO/IEC 29128 (проект) «Информационные технологии. Методы и средства обеспечения безопасности. Верификация криптографических протоколов»;

– ISO/IEC 29147 (проект) «Информационные технологии. Методы и средства обеспечения безопасности. Обнаружение значимых уязвимостей»;

– ISO/IEC 29193 (проект) «Информационные технологии. Методы и средства обеспечения безопасности. Принципы и методы инжиниринга безопасности систем»;

– ISO/IEC TR 14516:2002 «Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по использованию и управлению службами доверительной третьей стороны»;

– ISO/IEC 15816:2002 «Информационные технологии. Методы и средства обеспечения безопасности. Информационные объекты безопасности для управления доступом»;

– ISO/IEC 15945:2002 Информационные технологии. Методы и средства обеспечения безопасности. Спецификация служб TTP для поддержки применения электронных подписей;

– ISO/IEC 18028 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационной технологии». Включает в себя следующие части: часть 1 «Менеджмент сетевой технологии»; часть 2 «Архитектура обеспечения безопасности сети»; часть 3 «Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности»; часть 4 «Обеспечение безопасности удаленного доступа»; часть 5 «Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем»;

– ISO/IEC 18043:2006 «Информационные технологии. Методы и средства обеспечения безопасности. Выбор, применение и операции систем обнаружения вторжения»;

– ISO/IEC TR 18044:2004 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

– ИСО/МЭК 24762:2008 «Информационная технология. Методы и средства

обеспечения безопасности. Руководство по услугам по восстановлению информационно-коммуникационных технологий после бедствия»;

– ISO/IEC 27033 «Сетевая безопасность». Включает в себя следующие части: часть 1 «Обзор и общие понятия»; часть 2 «Руководства по разработке и внедрению сетевой безопасности»; часть 3 «Эталонные сетевые сценарии – риски, технологии разработки и вопросы управления»; часть 4 «Обеспечение безопасности межсетевых соединений с применением шлюзов безопасности – риски, технологии разработки и вопросы управления»; часть 5 «Обеспечение безопасности межсетевых коммуникаций с применением виртуальных частных сетей – риски, технологии разработки и вопросы управления»; часть 6 «Совпадение IP-адресов»; часть 7 «Беспроводные коммуникационные технологии»;

– ISO/IEC 27032 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Руководства по кибербезопасности»;

– ISO/IEC 27034 «Безопасность приложений». Включает в себя следующие части: часть 1 «Обзор и общие понятия»; часть 2 «Структура организации нормативного обеспечения»; часть 3 «Процесс менеджмента безопасности приложений»; часть 4 «Подтверждение безопасности приложений»; часть 5 «Структура данных средств управления безопасностью протоколов и приложений»;

– ISO/IEC 27035 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

– ISO/IEC 27036 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Руководства по обеспечению безопасности при аутсорсинге»;

– ISO/IEC 27037 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору и /или получению и хранению свидетельств, представленных в цифровой форме»;

– ISO/IEC 24745 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Защита биометрических шаблонов»;

– ISO/IEC 24761:2009 «Информационные технологии. Методы защиты. Контекст аутентификации для применения в биометрических технологиях»;

– ISO/IEC 29100 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности»;

– ISO / IEC 29101 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Эталонная архитектура обеспечения приватности»;

– ISO/IEC 29115 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Доверие к аутентификационным атрибутам»;

– ISO/IEC 29146 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Основы менеджмента доступа»;

– ISO/IEC 29190 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Модель зрелости возможностей обеспечения приватности»;

– ISO/IEC 29191 (проект) «Информационная технология. Методы и средства обеспечения безопасности. Требования по взаимной анонимности при депонировании идентификационных атрибутов».

Приложение 2

Подходы к формированию нормативного обеспечения системы информационной безопасности организации

Комплексный подход к обеспечению ИБ, предполагающий последовательное и взвешенное использование правовых, организационных, программнотехнических и других мер обеспечения ИБ на единой концептуальной и методической основе, должен сформировать и поддержать адекватный потребностям бизнеса организации уровень ее информационной безопасности.

Согласованность, целенаправленность и планомерность деятельности по обеспечению ИБ может быть достигнута только при надлежащем нормативном закреплении (документировании) ожиданий руководства и правил осуществления деятельности в организации. Документы позволяют отразить и формализовать необходимые нормы, которые далее могут быть единообразно доведены до каждого работника организации в виде правил и требований ИБ, которыми он должен руководствоваться в своей производственной деятельности, а также порядка контроля их соблюдения.

Для того чтобы сформировать и обеспечить эффективную поддержку полноценной и непротиворечивой системы внутренних документов обеспечения ИБ организации, необходимо представлять и понимать суть возможной структуры комплекса таких документов. Например, видение Банка России относительно возможной эталонной структуры нормативного обеспечения системы ИБ организации отражено в рекомендациях в области стандартизации Банка России РС БР ИББС-2.0-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0». Определенная данными рекомендациями структура нормативного обеспечения системы информационной безопасности организации банковской системы Российской Федерации приведена на рис. 1.

Рис. 1. Эталонная структура нормативного обеспечения системы информационной безопасности организации БС РФ

Такая структура документов позволяет формализовать любую необходимую деятельность на всех уровнях управления в организации. Подобная структура документов, относящихся к деятельности по обеспечению ИБ, рекомендуется и Международной группой пользователей системы менеджмента информационной безопасности (ISMS International User Group).

Представленную структуру внутренних документов обеспечения ИБ можно рекомендовать любой организации. Далее кратко остановимся на целях и назначении документов каждого из уровней предложенной структуры.

К документам первого уровня относятся документы, содержащие положения (правила, принципы, нормы) политики ИБ организации, т. е. формулировки высокоуровневого видения сути проблемы в области ИБ руководством организации и определения позиции организации в их решении. Таким образом, в политике ИБ организации, как правило, определяются

высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ. Действие такого документа обычно распространяется на все подразделения и всех работников организации.

К документам второго уровня относятся документы, содержащие положения так называемых «частных» политик ИБ, т. е. документы, детализирующие положения основополагающей политики ИБ организации в отношении одной или нескольких областей ИБ, а также в отношении отдельных видов и технологий деятельности организации. Эти документы, как правило, определяют цели, назначение, состав работ (процессов деятельности), необходимых как для реализации деятельности в той или иной области ИБ, так и для реализации отдельной технологии обеспечения ИБ, а также необходимые требования в рамках реализуемой деятельности. Количество частных политик зависит от номенклатуры необходимых видов деятельности по обеспечению ИБ, определенных основополагающей политикой ИБ организации. Частные политики ИБ определяют деятельность лиц или группы лиц, ответственных за реализацию комплекса мероприятий соответствующей области ИБ.

К документам третьего уровня относятся документы, содержащие требования ИБ, применяемые к операционным процедурам (порядку выполнения действий или операций) обеспечения ИБ. Данные документы содержат правила и параметры, устанавливающие способы осуществления и выполнения конкретных видов работ в рамках процессов, связанных с ИБ технологических процессов, реализуемых в организации. Кроме того, данные виды документов могут содержать различного рода ограничения по выполнению отдельных действий, связанных с реализацией защитных мер в используемых технологических процессах (технические задания, регламенты, порядки, инструкции). В документах третьего уровня можно выделить следующие группы документов.

– Документы, регламентирующие реализацию процессов. Определяют роли, задействованные в реализации конкретных процессов, а также порядок действий исполнителя каждой роли и взаимодействие между ними. К этим документам можно отнести различного рода регламенты, порядки. Данные документы можно считать документами должностных лиц, ответственных за вверенные им участки работ по обеспечению ИБ. Введение в действие в организации таких документов позволяет упорядочить деятельность, что создает условия для ее эффективного контроля. Кроме того, к данной группе документов можно отнести документы, содержащие различного рода ограничения (требования) по выполнению отдельных действий, связанных с реализацией защитных мер в используемых технологических процессах. Такие документы, как правило, необходимы там, где затруднительно формализовать реализуемую деятельность. К этим документам можно отнести различные положения, своды правил, требования.

– Документы, определяющие порядок действий конкретного должностного лица в рамках реализации своей роли в конкретном процессе. Это уже документы исполнителей ролей в рамках процессов деятельности. К ним относятся различного рода инструкции, маршрутные карты и т. п. Кроме порядка действий исполнителя определенной роли в таком документе могут быть определены и требования, которые данное должностное лицо должно выполнять в процессе своей деятельности.

К документам четвертого уровня, относятся свидетельства выполненной деятельности по обеспечению ИБ. Данные документы отражают результаты (промежуточные и окончательные) реализации процессов деятельности. Обычно к ним относятся различные журналы (бумажные и электронные), отчеты, протоколы и т. д. Данные документы необходимы в основном для осуществления контрольной деятельности, а также для обеспечения условий для восстановления хода работ в рамках расследования и иных случаях. С точки зрения контрольных органов отсутствие подобных свидетельств, даже при наличии регламентирующих деятельность документов, может означать, что регламентированная деятельность либо реализуется произвольным образом, в том числе и с

нарушениями, либо не реализуется вовсе.

Не редки случаи, когда в организациях придается слабое значение вопросам обеспечения ИБ, включая нормативное обеспечение данного направления деятельности. В таких ситуациях отсутствие документов «верхнего» уровня, определяющих цели и задачи обеспечения ИБ организации, как показано на рис. 2, означает, что руководство организации не ощущает потребности в ИБ и не будет потребителем результатов этой деятельности. В таких условиях работа службы обеспечения информационной безопасности организации не востребована и не ясна для руководства организации и подразделений бизнеса. В результате руководство организации воспринимает риски ИБ как риски бизнеса и реагирует на них не методами улучшения качества и стабилизации информационных процессов, а через экономические, финансовые, юридические, организационные, контрольные и иные механизмы. В отдельных случаях это может эффективным (перенос рисков на клиентов/контрагентов и т. п.), но чаще подобные меры более сложны, чем меры реагирования ИБ на риски в информационной сфере.

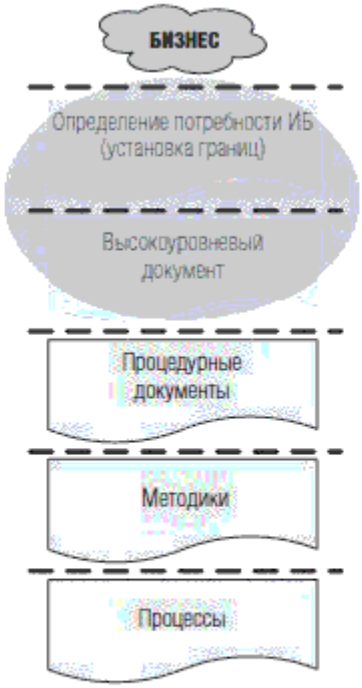


Рис. 2. Разрыв в архитектуре управления из-за отсутствия необходимых документов «верхнего» уровня

Отсутствие же документов «нижнего» уровня, как показано на рис. 3, означает, что не регламентированы процессы операционной деятельности по обеспечению ИБ организации. Но это может и не означать, что необходимая деятельность не реализуется. Деятельность может осуществляться, только она может иметь существенную вариативность и непредсказуемость по результатам, быть затруднительной для контроля и анализа. Такая ситуация наиболее типична для небольших и малых организаций. В этом случае руководство организации опирается на опыт и знания специалистов высокой квалификации. Таким образом, процессы могут быть организованы должным образом и будут на нижнем уровне успешно реализовываться, документироваться, но отсутствие заранее определенного интерфейса приведет к тому, что отчетные данные процессов обеспечения ИБ на верхнем уровне не смогут быть эффективно использованы. Подобная ситуация также чревата тем, что с уходом специалистов (смена работы, длительные командировки и т. п.) идет потеря операционной технологии (утрата «носителя» знаний). В отдельных случаях такие потери могут быть крайне чувствительными.

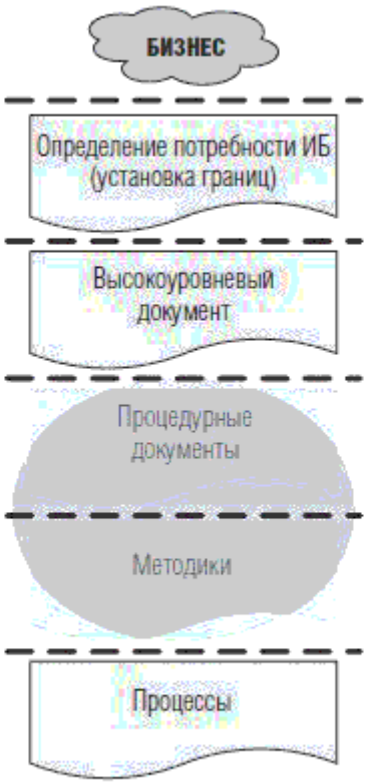


Рис. 3. Разрыв в архитектуре управления из-за отсутствия документов «нижнего» уровня

Анализ международной и российской практики, отраженной в международных и национальных стандартах, позволяет сформулировать следующий примерный перечень областей ИБ, которые могут быть охвачены положениями внутренних документов обеспечения ИБ организации:

– назначение и распределения ролей ИБ;
– обеспечение доверия к персоналу;
– менеджмент рисков ИБ;
– менеджмент инцидентов ИБ;
– обеспечения ИБ на стадиях жизненного цикла автоматизированных систем;
– управление доступом;
– защита от вредоносных программ;
– обеспечение ИБ при использования ресурсов электронной почты и сети Интернет;
– криптографическая защита информации;
– обеспечение «чистых столов» и «чистых экранов»;
– самооценка состояния ИБ;
– аудит ИБ.

В конкретной организации состав областей ИБ и перечень технологий обеспечения ИБ, в отношении которых формируется система документов, может отличаться от приведенного выше перечня.

Необходимо отметить, что не для каждой области ИБ может оказаться возможным построение полной (идеальной) пирамиды нормативных документов. В качестве примера можно привести правило (политику) так называемых «чистых столов». Обычно подобные правила отражают в частной политике или в инструкциях персонала. Таким образом, разработка документов по обеспечению ИБ требует взвешенного подхода и во многом зависит от сложившихся в организации принципов управления и контроля.

Далее на примере деятельности по менеджменту инцидентов ИБ (рис. 4) рассмотрим примерную (возможную) структуру нормативно-методического обеспечения для этого вида деятельности.

В данном примере мы исходим из предположения того, что руководством организации в основополагающем документе «Политика информационной безопасности организации» определены и утверждены высокоуровневые цели, содержание и основные направления деятельности по менеджменту инцидентов ИБ. В этом случае «частная» политика менеджмента инцидентов ИБ определяет требования к процессам: мониторинга инцидентов ИБ; сбора информации об инцидентах ИБ; анализа и обработки инцидентов ИБ.

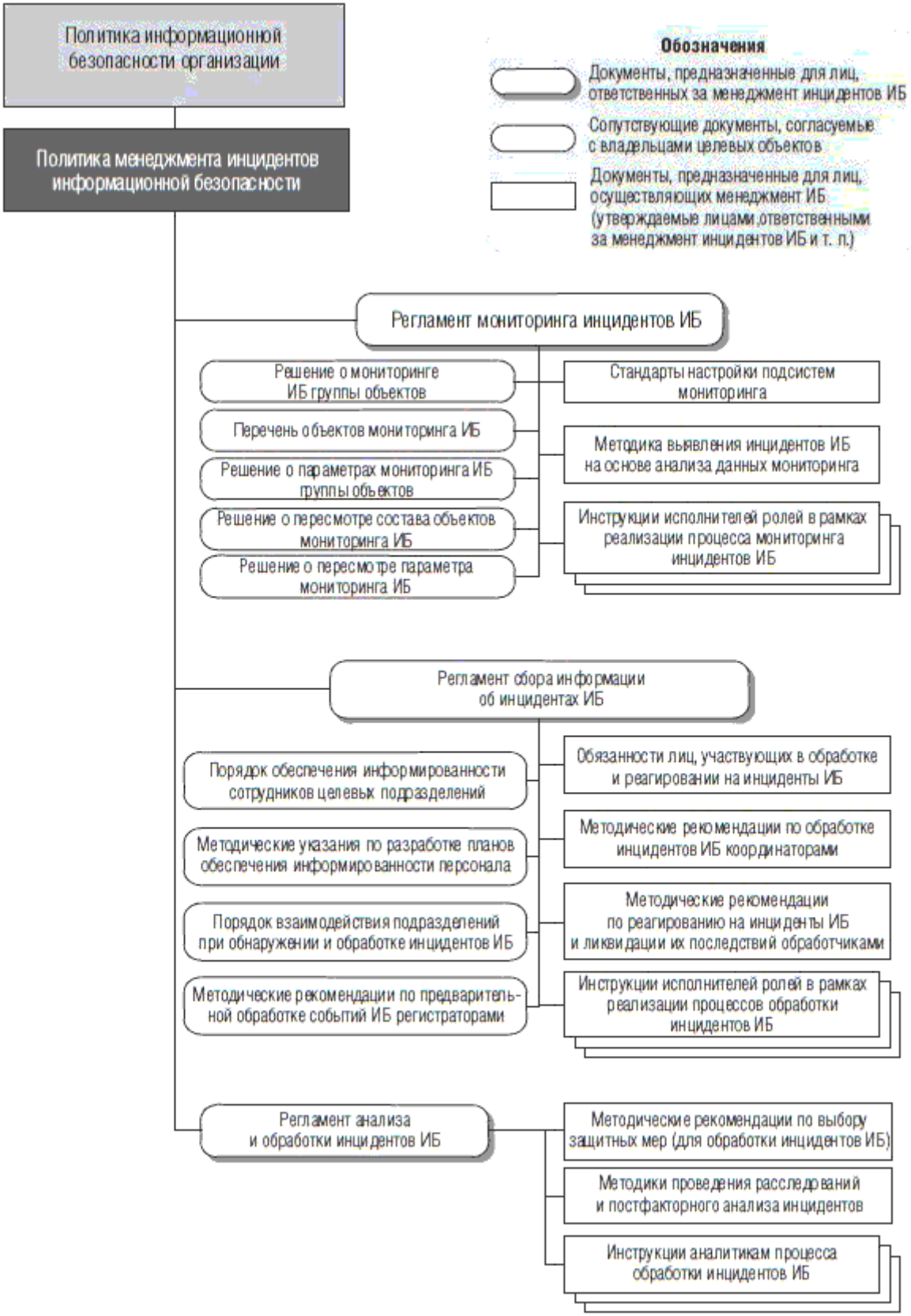


Рис. 4. Примерная структура нормативно-методического обеспечения деятельности по менеджменту инцидентов ИБ

В примерной структуре не показаны документы, составляющие свидетельства выполненной деятельности, так как их состав напрямую зависит от реализуемых технологий и состава используемых продуктов и систем обеспечения ИБ.

При разработке внутренних нормативных документов в области обеспечения ИБ

необходимо обеспечить, чтобы разрабатываемые документы:

– носили не рекомендательный, а обязательный характер;

– были выполнимыми и контролируемыми, не рекомендуется включать в состав этих документов положения, контроль реализации которых затруднен или невозможен;

– были адекватны требованиям и условиям ведения деятельности (включая угрозы и риски ИБ), в том числе в условиях их изменчивости;

– не противоречили друг другу.

Оформление и содержание документов по обеспечению ИБ должны соответствовать установленным в организации нормам к содержанию и оформлению внутренних документов. Тем не менее в отношении содержания политики информационной безопасности организации и в отношении частных политик ИБ целесообразно руководствоваться положениями ГОСТ Р ИСО/МЭК 17799 «Информационная технология. Практические правила управления информационной безопасностью». В соответствии с указанным стандартом в политику ИБ организации рекомендуется включать следующие положения:

– определение информационной безопасности организации, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

– изложение целей и принципов информационной безопасности, сформулированных руководством;

– краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

– соответствие законодательным требованиям и договорным обязательствам;

– требования в отношении обучения вопросам безопасности;

– предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

– управление непрерывностью бизнеса;

– ответственность за нарушения политики безопасности;

– определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

– ссылки на документы, дополняющие политику информационной безопасности, например, частные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Пример основополагающей политики ИБ организации приведен на рис. 5.

Политика информационной безопасности организации

1 Общие положения

1.1 Область действия

Действие данной политики распространяется на все защищаемые информационные активы организации, а также технологии обработки информации.

Положения данной политики обязательны для исполнения руководителями организации и ее подразделений, работниками (временными и постоянными), сторонними организациями, имеющим доступ к информационным активам организации.

1.2 Назначение

Политика определяет правила и ответственности обеспечения информационной безопасности, а также определяет развивающие ее частные политики, стандарты, документы по процессам информационной безопасности.

Реализация данной политики предназначена для достижения следующих целей:

— обеспечения необходимой доступности информационных ресурсов организации в целях обеспечения непрерывности ее бизнеса;

— обеспечения целостности информационных ресурсов организации в целях обеспечения требуемой поддержки деятельностей организации в информационной сфере, включая задачи принятия решений;

— …

1.3 Причины

Информационные активы являются одним из наиболее ценных активов организации и эффективность деятельности организации значительным образом зависит от их безопасности. Как и все остальное, информационные активы должны быть защищены от любого возможного неправомочного использования.

Однако существуют угрозы, которые могут нарушить безопасность деятельностей организации. К ним относятся (но этим не ограничивается):

— неправомочные действия работников организации;

— …

Данный документ определяет меры, направленные на защиту информационных активов организации с целью минимизации информационных рисков.

Действие документа распространяется на все филиалы организации. Каждый филиал ответственен за реализацию данной политики.

2 Положения политики

Все информационные активы организации должны защищаться в соответствии с уровнем их важности для бизнеса организации и степенью их конфиденциальности (для информационных ресурсов).

Информационные активы организации должны быть классифицированы в соответствии с их важностью для бизнеса организации.

Применяемые защитные меры должны быть адекватны установленной классификационной категории.

Ответственность за классификацию информационных активов возлагается на назначенное лицо, ответственное за конкретный информационный актив.

— …

3 Контроль

В организации должен обеспечиваться мониторинг соответствия данной политике. Кроме того, соответствие данной политике должно периодически подтверждаться аудитом и докладываться высшему руководству организации.

Руководители подразделений несут ответственность за то, что:

— применяемые меры обеспечения информационной безопасности соответствуют данной политике;

— …

Нарушения данной политики должны быть предметом расследований, по результатам которых должны быть приняты соответствующие меры.

4 Связанные политики и стандарты

Требования настоящей политики детализируются необходимыми частными политиками, стандартами и документами по процессам информационной безопасности, которые обеспечивают поддержку и уточнение настоящей корпоративной политики информационной безопасности.

5 Ответственное лицо

Указывается ответственное лицо.

6 Пересмотр (период актуализации)

Период пересмотра политики составляет 12 месяцев.

В случае внедрения новых банковских технологий пересмотр должен начаться непосредственно после принятия соответствующего решения.

Рис. 5. Пример основополагающей политики ИБ организации

При разработке структуры частных политик целесообразно исключать повторения одинаковых правил в различных частных политиках. При необходимости повторения в какой-либо частной политике ИБ правила или группы правил, содержащихся в другой (существующей) частной политике ИБ, целесообразно использовать ссылку на

существующую частную политику ИБ. Например, включение в политику обеспечения ИБ какого-либо технологического процесса требований по антивирусной защите целесообразно осуществить в виде ссылки на политику антивирусной защиты (при ее наличии).

К инструкциям, руководствам (регламентам), методическим указаниям по обеспечению ИБ, как правило, предъявляются повышенные требования четкости и ясности изложения текста. Документы этого уровня, в отличие от документов вышестоящего уровня, описывают конкретные приемы и порядок действий сотрудников для решения определенных им (например, ролью) задач либо конкретные ограничения.

Рекомендуется, чтобы инструкции, руководства (регламенты), методические указания по обеспечению ИБ содержали:

– определение субъекта (субъектов), деятельность которых регламентируется инструкцией, и /или наименование деятельности (процесса), которая описывается инструкцией;

– ресурсы, необходимые для выполнения деятельности (процесса);

– детальное описание выполняемых операций, включая накладываемые ограничения, и результат выполнения операций;

– обязанности субъекта (субъектов) в рамках выполнения регламентируемой деятельности;

– права и ответственность субъекта (субъектов).

Недостаточно только разработать и ввести в действие документы по обеспечению ИБ. Документы должны иметь поддержку их жизненного цикла и быть актуальными осуществляемой организацией деятельности, а также внутренним и внешним условиям реализации этой деятельности. Менеджмент документов по обеспечению ИБ направлен на обеспечение разработки, учета, использования, хранения, проверки, обновления (поддержание актуального состояния) и изменения документов по обеспечению ИБ организации.

Менеджмент документов по обеспечению ИБ должен учитывать существующие требования законодательных актов и нормативных документов Российской Федерации, нормативных актов органов-регуляторов и внутренних документов организации. Документы должны сохраняться удобочитаемыми, легко идентифицируемыми и доступными. В организации должны существовать и быть документированы деятельности, направленные на идентификацию, хранение, защиту, поиск, обеспечение времени хранения документов, правила по их утилизации.

Модель менеджмента документов по обеспечению ИБ, гармонизированная с моделью менеджмента ИБ, определенной стандартом ГОСТ Р ИСО/МЭК 27001, приведена на рис. 6.

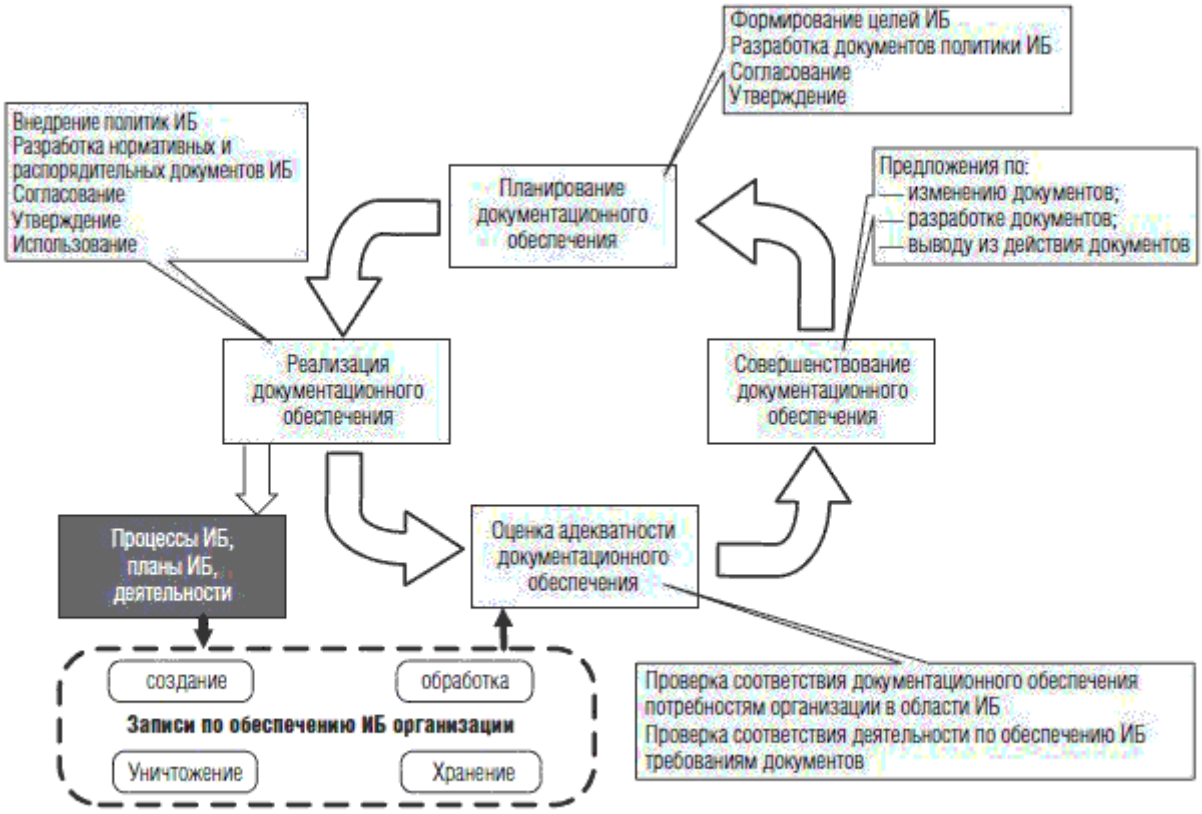


Рис. 6. Модель менеджмента документов по обеспечению ИБ

На этапе «Планирование документационного обеспечения» реализуются следующие процессы менеджмента документов по обеспечению ИБ:

– определение потребностей организации по обеспечению ИБ;

– разработка, согласование и утверждение основополагающей (корпоративной) политики ИБ организации и частных политик ИБ;

– разработка, согласование и утверждение документов, содержащих описания основных процессов обеспечения ИБ (например, менеджмент инцидентов ИБ, менеджмент рисков ИБ, оценка ИБ организации, обучение и осведомление персонала и др.).

К разработке и согласованию корпоративной политики ИБ и частных политик ИБ организации должны привлекаться представители следующих служб организации, ответственных за реализацию управленческих, основных производственных и вспомогательных процессов организации, связанных с ее информационной сферой:

– лица из состава высшего руководства организации;

– профильных (основных производственных) подразделений;

– службы информатизации;

– службы безопасности (информационной безопасности).

Все документы, составляющие политику ИБ организации, должны быть согласованы, введены в действие и учтены в соответствующем реестре. Корпоративная политика ИБ должна быть утверждена руководителем организации (например, председателем, генеральным директором, президентом, руководителем филиала). Частные политики ИБ могут быть утверждены руководителем организации или его заместителем по вопросам ИБ.

Документы, содержащие требования информационной безопасности к процессам, могут быть утверждены руководителем организации, его заместителем по вопросам ИБ или иными должностными лицами, в компетенцию которых входят вопросы, отраженные в этих документах.

В организации должно быть определено лицо (или лица), ответственное (или

ответственные) за реализацию политики ИБ организации, ее поддержку в актуальном состоянии, включающее пересмотр политики в соответствии с установленным в организации порядком.

В организации должно быть определено лицо (или лица), ответственное (или ответственные) за контроль реализации политики ИБ организации. Как правило, не допускается выполнение этими же сотрудниками организации функций по обеспечению реализации политики ИБ организации.

На этапе «Реализация документационного обеспечения» осуществляются следующие процессы менеджмента документов по обеспечению ИБ:

– внедрение в деятельность организации принятых документов политики ИБ, разработанных на этапе «Планирование документационного обеспечения» и содержащих описания основных процессов обеспечения ИБ;

– разработка, согласование и утверждение документов второго и третьего уровней нормативного обеспечения ИБ организации (см. рис. 1);

– внедрение утвержденных документов второго и третьего уровней;

– управление регистрационными данными о реализации требований нормативных актов по обеспечению ИБ организации, являющихся свидетельствами реализации процессов и задач обеспечения ИБ.

Ответственность за организацию работ в соответствии с требованиями, определенными документами второго и третьего уровня, возлагается решением руководства организации посредством соответствующих распорядительных документов.

Все документы второго и третьего уровней должны быть согласованы, введены в действие и учтены в соответствующем реестре (каталоге), который может быть организован и размещен в электронном виде во внутрикорпоративной системе.

Документы, содержащие требования информационной безопасности к процессам, могут быть утверждены руководителем организации, его заместителем по вопросам ИБ или иными должностными лицами, в компетенцию которых входят вопросы, отраженные в этих документах.

Документы, содержащие требования информационной безопасности к задачам, могут быть утверждены лицами, ответственными за реализацию соответствующих процессов ИБ.

На этапе «Оценка адекватности документационного обеспечения» реализуются следующие процессы менеджмента документов по обеспечению ИБ:

– проверка соответствия деятельности по обеспечению ИБ действующим документам по обеспечению ИБ;

– проверка адекватности самих документов реальным потребностям организации по обеспечению ИБ.

Проверка может производиться как путем проведения мониторинга, так и путем проведения внутреннего аудита ИБ (внутреннего контроля) или внешнего аудита ИБ.

При проведении аудита ИБ положения документов политики ИБ, нормативных документов по обеспечению ИБ являются критериями аудита ИБ, а записи – свидетельствами реализации требований.

На этапе «Совершенствование документационного обеспечения» на основе результатов проведения мониторинга, а также внешнего или внутреннего аудита ИБ производится внесение изменений (актуализация) в соответствующие документы, разработка новых, вывод из действия устаревших.

Если же рассмотреть жизненный цикл отдельного документа, то в нем также выделяются отдельные стадии, которые в свою очередь коррелируются со стадиями жизненного цикла всей системы документов. В качестве примера можно рассмотреть модель жизненного цикла документа, приведенную в международном стандарте ISO 11442 Technical product documentation. Document management и представленную на рис. 7.

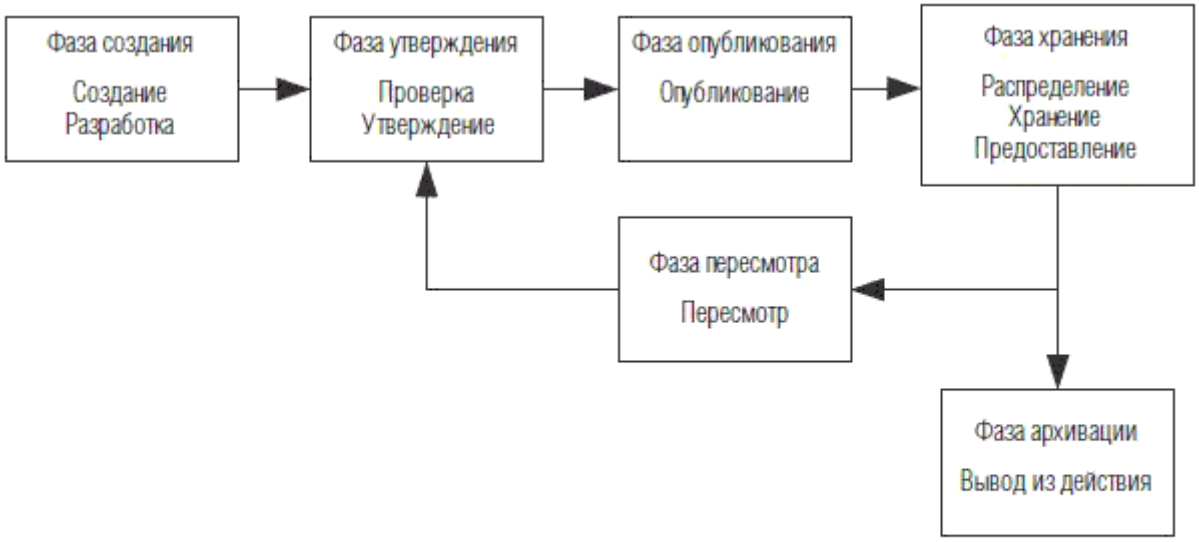


Рис. 7. Фазы жизненного цикла документа

Фаза, в которой устанавливается фактическое содержание документа, является фазой разработки. По решению разработчика о завершении разработки документа должна быть инициирована фаза утверждения. Данная фаза характеризуется статусом документа «в рассмотрении». Документ с указанным статусом все еще находится в собственности разработчика, и в отношении его использования действуют те же ограничения. Опубликование является независимой деятельностью по отношению к утверждению. Следовательно, в целях согласования с выпуском других документов в рамках проекта должен быть определен срок опубликования документа. Фаза, в которой опубликованные документы находятся на хранении и доступны авторизованным пользователям для чтения и копирования, называется фазой хранения. Фаза пересмотра подразумевает собой получение копии хранящегося документа, передачу на пересмотр, а также присвоение ей статуса «в подготовке». Фаза архивации обуславливается перемещением документов из хранилища действующих документов в архив для хранения на установленный период.

Рассмотренная модель жизненного цикла документа может быть взята организациями за основу при формировании и внедрении системы менеджмента документов по обеспечению ИБ.

Обзор современных средств управления доступом (ЗАО «Инфосистема Джет»)

Алексей Лаврухин, директор по развитию
Вячеслав Петрухин, консультант
Центр информационной безопасности
Компания «Инфосистемы Джет»

Управление доступом относится к числу приоритетных задач обеспечения информационной безопасности. При всей важности встроенных и наложенных средств защиты информации эффект от их использования может быть сведен на нет, если политика предоставления доступа в организации является неоптимальной и непродуманной и основывается на устаревших средствах управления доступом. По этим причинам внедрение современных средств управления доступом является одним из основных направлений деятельности по обеспечению защиты информации компании «Инфосистемы Джет».

Недостатки традиционного подхода к управлению доступом

Одна из особенностей традиционного управления доступом заключается в том, что для бизнеса информационная система является в значительной степени «черным ящиком»: сотрудники бизнес-подразделений не могут проконтролировать, какие права доступа назначаются администраторами систем сотрудникам и какие привилегии они в результате имеют.

Усугубляет ситуацию и то, что ИТ-инфрастуктура организации, как правило, состоит из множества различных информационных систем, большинство из которых имеет свое собственное хранилище учетных записей и связанных с ними привилегий. Эти политики могут значительно различаться, а управление учетными записями становится трудоемкой задачей. В результате невозможно представить полную картину прав доступа сотрудников и тем более получать такую информацию оперативно и регулярно.

Выполнение операций с учетными записями является по большей части механической работой, которая может быть автоматизирована. Традиционное ручное управление учетными записями, особенно в случае неподконтрольности результата, чревато как случайными, так и умышленными ошибками, которые могут быть выявлены лишь спустя значительное время или не выявлены совсем. Также ручное управление доступом приводит к задержкам предоставления или изменения доступа, вследствие чего увеличивается время вынужденного простоя, если сотрудник не может выполнять свои служебные обязанности или риски безопасности, если по каким-то причинам права доступа сотрудника в данный момент являются избыточными.

На практике реализация единой политики доступа к информационным ресурсам затрудняет поиск компромисса между удобством и безопасностью. В частности, если пользователь имеет доступ к пяти информационным системам, он вынужден помнить различные пароли, отвечающие всем требованиям сложности. А если сделать смену пароля обязательной хотя бы раз в три месяца, то самой частой задачей отдела системного администрирования, вероятно, будет восстановление забытых паролей, а пользователи будут записывать пароли на стикерах в текстовых файлах.

Средства предотвращения утечек информации (Data Leak Prevention – DLP) также значительно снижают удобство использования информационных ресурсов. Так, например, стандартными мерами по предотвращению распространения конфиденциальной информации являются запрет на использование USB-носителей и контентная фильтрация исходящего почтового трафика. Эти меры затрудняют обмен информацией даже в том случае, когда ее передача легитимна (например, в случае отправки конфиденциальных документов контрагентам), и не позволяют управлять доступом к служебной информации за пределами периметра. Впрочем, и внутри периметра отследить и предотвратить доступ к конфиденциальной информации на уровне файлов с помощью стандартных DLP-решений крайне сложно или даже невозможно.

Современные средства управления доступом

Основные тенденции, которые прослеживаются в развитии средств управления доступом, – повышение прозрачности соответствующих процессов и их передача под контроль бизнес-подразделений.

Эти тенденции, а также сложность администрирования разнородных хранилищ учетных записей привели к появлению информационных систем **Identity Management (IdM)** , одними из основных задач которых являются централизация и автоматизация процессов управления доступом. IdM-система подключается к «доверенному источнику», которым чаще всего является система кадрового учета для получения данных о сотрудниках (прием на работу, изменение должности, увольнение и т. д.), и к «целевым системам» – информационным системам и бизнес-приложениям организации. На основании данных

доверенного источника IdM-система запускает процессы управления учетными записями и правами доступа, которые могут включать согласования, эскалации и делегирование отдельных функций этих бизнес-процессов. Такой подход позволяет реализовать принцип разделения полномочий в управлении доступом (Segregation of Duties – SoD), согласно которому каждый процесс должен иметь более одного участника, что значительно снижает риск предоставления избыточных полномочий. На основании данных доверенного источника IdM-система запускает процессы управления учетными записями и правами доступа, а также контроля привилегий пользователей в целевых системах и формирования отчетов, которые могут включать согласования, эскалации и делегирование отдельных функций этих бизнес-процессов.

Другой тенденцией является создание единой модели ролевого управления доступом (Role Based Access Control – RBAC) в рамках всех информационных систем организации. Реализующие такой подход средства (**Role Management**) могут являться как частью IdM-системы, так и отдельным продуктом. Использование средств Role Management позволяет описать конкретные привилегии пользователей в терминах «ИТ-ролей» (например, «доступ на чтение к сетевому каталогу подразделения N») и сгруппировать их в так называемые бизнес-роли, которые могут соответствовать связке должности плюс подразделение сотрудника или выполняемым им обязанностям. Назначение бизнес-роли сотруднику в системе IdM приведет к изменению его прав доступа в целевых системах.

Средствами, позволяющими выполнить требования безопасности к авторизации пользователей в информационных системах, являются решения, обеспечивающие однократную аутентификацию (**Single Sign-On – SSO**). Клиентская часть SSO устанавливается на рабочую станцию пользователя и после его авторизации в корпоративном каталоге получает из него информацию об учетных данных конкретного пользователя в различных информационных системах. При попытке авторизации пользователя в каком-либо бизнес-приложении компонент SSO распознает окно ввода логина и пароля и подставляет их в соответствующие поля. Для вебприложений аналогичные задачи выполняются решениями Access Management. Интеграция решений Single Sign-On и Access Management с системой Identity Management позволяет реализовать сложные политики управления паролями и доступом к приложениям и одновременно увеличить удобство использования информационных ресурсов организации. Соответствующий всем требованиям сложности пароль устанавливается в бизнес-приложении IdM-системой и записывается в хранилище систем SSO и Access Management. Далее автоматически пароль меняется через заданные промежутки времени. При этом пользователю достаточно помнить один пароль от корпоративного каталога, необходимый для авторизации на рабочей станции. Максимального уровня безопасности можно добиться при использовании двухфакторной аутентификации для доступа пользователя в домен сети предприятия.

Современные средства, позволяющие управлять доступом к информации на уровне файлов, тем самым позволяющие расширить функционал DLP-систем, относятся к классу **Information Rights Management – IRM** . Программное обеспечение IRM встраивается в средства создания носителей информации (офисные программы MS Office, системы документооборота и приложения, позволяющие экспортировать данные в файлы). При создании нового документа он может быть автоматически или вручную отнесен к одной из определенных категорий. Если содержимое документа было определено как конфиденциальное, оно «запечатывается» средствами IRM. Далее в зависимости от категории пользователя доступ к запечатанному файлу может быть ограничен или полностью закрыт. Технология запечатывания документа также не позволит скопировать его содержимое, в том числе и с помощью клавиши Print Screen, если это было запрещено при его создании. При этом с помощью сервера IRM сохраняется контроль доступа к файлам после их передачи по сети предприятия или за ее пределы: текущие права конкретного пользователя или целой группы могут быть изменены или полностью отозваны. Кроме того, на сервере сохраняется история работы с данным файлом, в том числе история неудачных

попыток его открытия, которая может быть использована для расследования инцидентов и предотвращения утечек информации.

Перечисленные средства позволяют контролировать доступ к информационным ресурсам на всех уровнях. В случае совместного использования они значительно повышают защищенность информационной безопасности организации и удобство использования информационных ресурсов, а также увеличивают прозрачность процессов управления доступом для бизнеса. Компания «Инфосистемы Джет» активно развивает это направление с 2006 г. В настоящее время специалистами компании реализовано большое количество проектов и накоплена компетенция, позволяющая реализовывать интеграционные проекты по управлению доступом любой сложности.

Россия, 127015, г. Москва,
ул. Б. Новодмитровская, д. 14, стр. 1
Тел.: (495) 411-76-01
Факс: (495) 411-76-02
E-mail: info@jet.msk.su
http://www.jet.msk.su

Приложение 3
(справочное)

Примеры метрик для измерения атрибутов

Менеджмент риска

Критический элемент	***1.1. Оцениваются ли периодически риски?***
Дополнительный (вспомогательный) вопрос	*1.1.2. Выполнятся ли оценки риска на регулярной основе или всякий раз, когда изменяются системы, средства или другие условия?*
Метрика	Процентное отношение систем, которые выполняют и документируют формальные оценки риска
Цель	Оценивать качественно число оценок риска, выполняемых относительно требований организации
Свидетельство реализации	*1. Проводит ли ваша организация текущую инвентаризацию систем ИТ?* _____ *ДА* _____*НЕТ* *2. Если да, то сколько систем в вашей организации (или организационном компоненте, если применимо)?* _____ *3. Из систем в вашей текущей инвентаризации сколько систем выполнили и документировали оценки риска в следующие временные интервалы? (Выбирайте для каждой системы; не учитывайте одну и ту же систему более чем в одном временном интервале.)* *За прошедшие 12 месяцев*_____ *За прошедшие 2 года*_____ *За прошедшие 3 года*_____ *4. Что касается какой-либо системы, которая претерпела оценку риска, перечислите количество систем согласно причине (причинам оценки:* *Планируемая оценка риска* _____ *Основное изменение в системной среде* _____ *Основные изменения в средствах (возможностях)* _____ *Изменение в других условиях (специфицируйте)* _____

	5. Что касается какой-либо системы, которая не претерпела оценку риска за последние три года, перечислите количество систем согласно причинам:. *Плановая оценка риска _____* *Нет политики _____ Нет ресурсов _____* *Степень системного уровня не требует _____* *Система ранее не определялась _____* *Новая система _____* *Другое (специфицируйте) _____*
Частота	Раз в полгода, ежегодно
Формула	На уровне организации. Суммируйте оценку риска на файле за каждый временной интервал (вопрос 3)/системы ИТ при инвентаризации (учетная база данных) (вопрос 2)[1]
Источник данных	Инвентаризация (запись) системы ИТ, которая включает все основные приложения и главные исполняющие системы; хранилище оценок риска
Идентификаторы (показатели)	Данная метрика вычисляет процентное отношение систем, которые претерпевают оценки риска за последние три года (что составляет обычно требуемый максимальный временной интервал для проведения оценок риска). Для установления оценки риска вычисляется количество систем, перечисляемых за каждый временной интервал. Сумма за три года должна равняться 100% всех требуемых систем. Системы, которые не подвергаются регулярным оценкам риска, вероятно, подвергаются угрозам. Вопрос 4 используется для подтверждения правильности причин для проведения оценок риска и для обеспечения того, чтобы учитывались все системы. Вопрос 5 включается для определения причины, по которой не выполнялись оценки риска. Определение причины направит внимание менеджмента непосредственно на соответствующие коррективные действия. Путем документации и отслеживания данных факторов могут выполняться изменения для улучшения функционирования посредствам модернизации политики безопасности, направление ресурсов или обеспечение того, чтобы системы оценивались на риск, как требуется

Безопасность, связанная с персоналом

Критический элемент	***6.1. Разделяются ли обязанности для обеспечения наименьшей привилегии и индивидуальной ответственности?***
Дополнительный (вспомогательный) вопрос	*6.1.3. Делятся ли чувствительные функции между различными физическими лицами?*
Метрика	Процентное отношение систем согласующихся с требованием разделения обязанностей
Цель	Измерить уровень согласования с требованием разделения обязанностей
Свидетельство реализации	*1. Проводит ли ваша организации текущую инвентаризацию систем ИТ?* *ДА _____ НЕТ _____* *2. Если да, то сколько систем имеется в вашей организации (компоненте организации)? _____*

	3. Сколько из данных систем требуют по плану их безопасности разделение обязанностей для обеспечения наименьшей привилегии и индивидуальной ответственности? *4. Сколько из данных систем проверяется на правильность (достоверность) для того, чтобы удовлетворять данному требованию?*
Частота	Ежегодно
Формула	Количество систем, оцениваемых на подчинение требованию (вопрос 4) / количество систем, которые формально признают требование (вопрос 3)
Источник данных	Хранилище оценок риска, хранилище C&A
Идентификаторы (показатели)	Результат для данной метрики должен приближаться к 100% для обеспечения того, чтобы все системы фактически принуждались к требованию разделения обязанностей. Низкое процентное отношение показывает подверженность высокому риску, поскольку одним и тем же фактическим лица разрешается выполнять транзакции, которые требуют разделения обязанностей

Обеспечение непрерывности бизнеса

Критический элемент	***9.1. Идентифицируются ли наиболее критические и чувствительные операции и поддерживающих их ресурсов вычислительных систем?***
Дополнительный (вспомогательный) вопрос	*9.1.1. Идентифицируются ли файлы критических данных и операции и документируются ли резервные копии файлов?*
Метрика	Процентное отношение файлов критических данных и операций с устанавливаемой частотой резервного копирования
Цель	Измерить угрозу риска вследствие недостаточных резервных копий
Свидетельство реализации	*1. Идентифицируются ли критические операции и файлы данных?* *ДА _____ НЕТ _____* *Не имеете критических данных/операций _____* *2. Если ответ на вопрос 1 отрицательный, то почему?* *Не знали требование _____* *Недостаток ресурсов _____* *Другое (объясните) _____* *3. Количество файлов критических данных и операций, идентифицируемых в качестве требующего резервного копирования _____* *4. Количество файлов критических данных и операций, идентифицируемых в качестве требующегося резервного копирования, для которого устанавливается и документируется частота резервного копирования _____* *5. Документируются ли резервные копии?* *ДА _____ НЕТ _____* *6. Регулярно ли копируются файлы (соответственно требованиям)?* *ДА _____ НЕТ _____* *7. Тестируются ли каждый раз резервные файлы на успешную полную передачу/копирование данных?* *ДА _____ НЕТ _____*
Частота	Ежегодно

Формула	Количество критических файлов с устанавливаемой частотой копирования (вопрос 4)/количество критических файлов, требующих резервного копирования (вопрос 3)
Источник данных	Ответы на вопросы NIST SP 800–26 и обзор
Идентификаторы (показатели)	Результаты данной метрики должны достигать 100%, показывая, что все файлы, требующие копирования, копируются в соответствии с установленным процессом резервного копирования. Регулярные резервные копии служат ключом для восстановления надежного результата для данной метрики, необходимо прежде всего идентифицировать критические файлы, которые требуют резервного копирования (вопрос 1). Затем система слежения должна записывать резервные копии (вопрос 5)

Критический элемент	***9.3. Имеются ли тестируемые план по чрезвычайным ситуациям/планы по аварийному восстановлению?***
Дополнительный (вспомогательный) вопрос	*9.3.3. Тестируется ли периодически и корректируется ли план соответствующим образом?*
Метрика	Процентное отношение систем, для которых тестировались планы по чрезвычайным ситуациям за последний год
Цель	Определить количество и процентное отношение планов по чрезвычайным ситуациям, тестируемых за прошедший год
Свидетельство реализации	*1. Поддерживает ли ваша организация текущую инвентаризацию систем ИТ? ДА _____ НЕТ _____* *2. Если да, то сколько систем есть в вашей организации (или компоненте организации)? _____* *3. Сколько планов по чрезвычайным ситуациям тестировалось в прошлом году? _____* *4. Записываются ли результаты тестирования? _____* *5. Сколько преобразований для планов было необходимо после тестирования? _____* *6. Сколько преобразований выло совершено? _____* *7. Сколько планов повторно тестировалось после выполнения преобразований? _____* *8. Сколько планов было завершено и утверждено менеджментом и затрачиваемыми сторонами после выполнения преобразований? _____*
Частота	Ежегодно
Формула	Количество тестируемых планов по чрезвычайным ситуациям (вопрос 3)/общее количество систем (вопрос 2)
Источник данных	Хранилище планов по чрезвычайным ситуациям
Идентификаторы (показатели)	Если данная метрика выдает низкое процентное отношение, она идентифицирует специфические системы для проверки исполнения и повторного тестирования, разработки плана по чрезвычайным ситуациям или анализа областей, в которых план по чрезвычайным ситуациям не модернизируется, как это необходимо

Управление доступом

Критический элемент	***10.1. Ограничивается ли доступ к ПО и аппаратному обеспечению?***
Дополнительный (вспомогательный) вопрос	*10.1.1. Существуют ли ограничения для тех, кто выполняет функции обслуживания и восстановления?*
Метрика	Процентное отношение систем, которые налагают ограничение на персонал по обслуживанию систем
Цель	Определить процентное отношение систем, которые имеют средства управления в функциях по обслуживанию систем для ограничения подвержению риску данных и возможности несанкционированной инсталляции компонентов в системе
Свидетельство реализации	*1. Сколько систем есть в вашей организации (или компоненте организации)? _____* *2. Сколько систем имеют ограничения для тех, кто исполняет функции по обслуживанию и восстановлению в системном ПО и аппаратном обеспечении? _____* *3. Сколько систем регистрируют функции обслуживания? _____* *4. Какая документация рассматривает ограничения обслуживания (проверка всего, что применяется):* *План безопасности систем _____* *Политика безопасности ИТ _____* *Системная конфигурация и операционные процедуры _____* *Другое (специфицируйте) _____* *5. Кому разрешается выполнять системное обслуживание и исправление (отметьте всех, кто имеет отношение):* *Инженеры внутренних систем _____* *Представители ведомственных внешних поставщиков ПО и аппаратного обеспечения _____* *Представители удаленных внешних поставщиков ПО или аппаратного обеспечения _____* *Другие (специфицируйте) _____* *6. Используются ли процедуры для управления удаленными услугами обслуживания, если диагностические процедуры или обслуживание выполняются через телекоммуникационные средства?* *ДА _____ НЕТ _____*
Частота	Ежегодно
Формула	Количество систем с ограничениями в обслуживающем персонале (вопрос 2/общее количество систем (вопрос 1)
Источник данных	Записи об обслуживании, документация по системной безопасности и операциям
Идентификаторы (показатели)	Данная метрика стремится, чтобы все системы ограничивали доступ к обслуживанию систем. Результат должен достигать 100% для полного соответствия. Обслуживающему персоналу разрешается специальный доступ и права к системе. Без средств управления, без ряда персонала и типу персонала с доступом к обслуживанию система является более открытой для несанкционированного доступа к обрабатываемым и сохраняемым данным и к инсталляции несанкционированных компонентов. Все системы должны иметь ограничения в доступе к обслуживанию для уменьшения подвержения данным рискам

Реализация программ обучения ИБ и осведомления ИБ

Критический элемент	***13.1. Проходят ли служащие адекватное обучение для выполнения обязанностей по безопасности?***
Дополнительный (вспомогательный) вопрос	*13.1.2. Обучаются ли служащие и документируется и контролируется ли професаональное развитие?*
Метрика	Процентное отношение служащих с значимыми обязанностями по безопасности, которые проходят специфицированное обучение
Цель	Измерять уровень экспертизы между назначаемыми ролями безопасности и обязанностями безопасности для специальных систем в организации
Свидетельство реализации	*1. Определяются ли значимые обязанности с помощью критериев квалификаций и документируют ли?* *ДА _____ НЕТ _____* *2. Поддерживаются ли записи о том, какие служащие имеют специализированные обязанности по безопасности?* *ДА _____ НЕТ _____* *3. Сколько служащих в вашей организации (или компоненте организации) имеют значимые обязанности по безопасности? _____* *4. Поддерживаются ли записи по обучению? (Записи по обучению показывают, что специфические служащие проходят обучение.)* *ДА _____ НЕТ _____* *5. Формулируют ли планы по обучению. Что необходимо специализированное обучение?* *ДА _____ НЕТ _____* *6. Сколько из тех, кто имеет значимые обязанности по безопасности, проходят необходимое обучение, формулируемое в их планах по обучению?* *_____* *7. Если весь персонал не проходит обучение, отметьте причины:* *Недостаточное финансирование _____* *Недостаток времени _____* *Нет курсов _____* *Служащие не регистрируются _____* *Другое (специфицируйте) _____*
Частота	Ежегодно как минимум
Формула	Количество служащих со значимыми обязанностями по безопасности, которые проходят обучение (вопрос 6)/количество служащих со значимыми обязанностями по безопасности (вопрос 3)
Источник данных	Записи или азы данных по обучению служащих, сертификаты о прохождении курсов
Идентификаторы (показатели)	Цель данной метрики 100%. Если персонал по безопасности не проходит соответствующего обучения, организация может не оснащаться для борьбы с новыми угрозами и уязвимостями. Специфические опции и инструментальные средства управления безопасностью быстро изменяются и развиваются. Непрерывное обучение поддерживает доступность необходимость обязательной информации по безопасности. Данная метрика может соотноситься с количеством инцидентов безопасности и количеством корректируемых уязвимостей для определения того, связывается ли количество обученного персонала безопасности с уменьшением определенных типов инцидентов и открытых уязвимостей и способствует ли этому

Обучение обеспечению информационной безопасности

Идентификация меры	
Название меры	Персонал, прошедший ежегодное обучение, направленное на повышение осознания информационной безопасности
Числовой идентификатор	Характерный для организации
Средство контроля или цель контроля	Средство контроля A. 8.2.2 [27001:2005]. Обучение, повышение осознания и компетентность. Все служащие организации и, где это уместно, подрядчики и пользователи третьей стороны должны получать соответствующее обучение, направленное на повышение осознания, и регулярные обновленные варианты политик и процедур организации, которые уместны для их рабочих функций
Назначение меры	Для оценки уровня осознания уязвимостей и угроз безопасности среди служащих и оценивания соответствия требованию ежегодного обучения, направленного на повышение осознания информационной безопасности
Проверяющий	Руководитель по обеспечению безопасности
Объекты измерения и атрибуты	
Объект измерения	База данных служащих
Атрибуты	Записи об обучении
Спецификация основной меры	
Основные меры	Число служащих, получивших ежегодное обучение, направленное на повышение осознания информационной безопасности. Число служащих, которые должны получать ежегодное обучение, направленное на повышение осознания информационной безопасности
Метод измерения	Подсчет полей/рядов, относящихся к ежегодному обучению, направленному на повышение осознания информационной безопасности, в журналах регистрации/реестрах, с пометкой «Получено»
Шкала	Шкала отношений

Спецификация производной меры	
Производная мера	Процентное отношение персонала, получившего ежегодное обучение, направленное на повышение осознания информационной безопасности
Метод измерения	Число служащих, получивших ежегодное обучение, направленное на повышение осознания информационной безопасности/Число служащих, которые должны получать ежегодное обучение, направленное на повышение осознания информационной безопасности × 100
Спецификация показателя	
Описание и пример показателя	Гистограмма, изображающая соответствие за несколько отчетных периодов, по отношению к пороговым значениям (красный, желтый, зеленый), определяемым аналитической моделью. Число отчетных периодов, которые будут использоваться в диаграмме, должно определяться организацией
Аналитическая модель	0–60% — красный; 60–90% — желтый; 90–100% — зеленый. В случае желтого, если не достигается, по крайней мере 10%-ного продвижения за квартал, оценка автоматически становится красной

Критерии принятия решений	Красный — требуется вмешательство, должен быть проведен причинный анализ для определения причин несоответствия и плохого функционирования. Желтый — за показателем следует внимательно наблюдать на предмет возможного сползания к красному. Зеленый — никаких действий не требуется
Интерпретация показателя	Характерная для организации
Эффекты / влияние	Красный и желтый — несоответствие системы менеджмента информационной безопасности. Красный указывает на серьезные проблемы с процессом обучения обеспечению информационной безопасности. Желтый — на возможные проблемы с процессом обучения обеспечению информационной безопасности
Причины отклонения	Характерные для организации. Потенциальные причины отклонения могут включать недостаточные финансовые ресурсы; неэффективный план обучения; отсутствие приверженности руководства; недостаток персонала и сложности с распределением рабочих смен, чтобы предусматривать время для обучения
Позитивные значения	Увеличивающиеся значения указывают на позитивные значения
Форматы отчетности	Гистограмма с цветовой кодировкой на основе критериев принятия решений. К этой гистограмме должно прилагаться краткое изложение того, что означает мера, и возможных действий руководства
Процедура сбора данных	
Частота сбора данных	Ежемесячно, в первый рабочий день месяца
Владелец информации	Ответственный за информационную безопасность и руководитель, отвечающий за обучение
Сборщик информации	Менеджмент обучения — отдел кадров
Инструментальные средства, используемые для сбора данных	Инструментальное средство запроса базы данных
Репозитарий собранных данных	Характерный для организации, может быть база данных или крупноформатная электронная таблица
Дата сбора	Являясь ежемесячной, она должна фиксироваться вместе с мерой
Процедура фиксирования данных	Характерная для организации
Мера действительна до…	Ежегодный пересмотр
Период анализа	Ежеквартально

Процедура анализа данных	
Частота сообщения данных	Ежеквартально
Лицо, сообщающее информацию	Руководители, отвечающие за систему менеджмента информационной безопасности
Источник данных для анализа	Записи кадровой службы
Инструментальные средства, используемые в анализе	Характерные для организации
Заказчик информации	Руководители, отвечающие за систему менеджмента информационной безопасности. Менеджмент безопасности. Менеджмент обучения

Приложение 4
ЗАО «ЕС-лизинг»

ЗАО «ЕС-лизинг» по заказу Банка России (БР) разработало систему обеспечения информационной безопасности коллективных центров обработки информации (КЦОИ) Банка России.

ЗАО «ЕС-лизинг» прошло экспертизу компании ООО «Пацифика» на соответствие требованиям и рекомендациям стандарта Банка России СТО БР ИББС-1.0-2006 «Обеспечение ИБ организацией банковской системы Российской Федерации. Общие положения». В результате экспертизы установлено, что система менеджмента информационной безопасности ЗАО «ЕС-лизинг» соответствует требованиям и рекомендациям стандарта Банка России СТО БР ИББС-1.0-2006 (уровень соответствия – второй).

ЗАО «ЕС-лизинг» имеет следующие лицензии Федеральной службы по техническому и экспертному контролю:

• лицензия (серия КИ 0028, № 001362) Федеральной службы по техническому и экспертному контролю на деятельность по разработке и (или) производству средств защиты конфиденциальной информации (регистрационный № 0269 от 11 апреля 2006 г., лицензия действительна до 11 апреля 2011 г.);

• лицензия (серия КИ 0028, № 001359) Федеральной службы по техническому и экспертному контролю на деятельность по технической защите конфиденциальной информации (регистрационный № 0463 от 11 апреля 2006 г., лицензия действительна до 11 апреля 2011 г.).

ЗАО «ЕС-лизинг» имеет следующие сертификаты соответствия от АНО «Центр независимой комплексной экспертизы и сертификации систем и технологий»:

• сертификат соответствия № ВР 08.1.2601-09, удостоверяющий, что система менеджмента качества, распространяющаяся на разработку, производство, гарантийное обслуживание (в том числе сопровождение) продукции в соответствии с классами ЕКПС 1210, 7010, 7015, 7030, 7031, отвечает требованиям ГОСТ Р ИСО 9001–2008 (ИСО 9001:2008), ГОСТ РВ 15.002-2003 и СРПП ВТ (действие сертификата с 16 декабря 2009 г. по 16 декабря 2012 г.);

• сертификат соответствия № SSAQ 032.3.1.0427, удостоверяющий, что система менеджмента качества применительно к проектированию, разработке, производству и

обслуживанию/поддержке/сопровождению соответствует требованиям ГОСТ Р ИСО 9001–2008 (ИСО 9001:2008 (действие сертификата с 16 декабря 2009 г. по 16 декабря 2012 г.).

Система обеспечения информационной безопасности КЦОИ Банка России

В ЗАО «ЕС-лизинг» разработана Система обеспечения информационной безопасности коллективных центров обработки информации (СОИБ КЦОИ) для обеспечения противодействия угрозам на 2-5-м уровнях. СОИБ КЦОИ БР является инфраструктурным решением и охватывает все автоматизированные системы и прикладные программные комплексы, функционирующие в КЦОИ Банка России.

СОИБ КЦОИ предназначена для обеспечения заданного уровня информационной безопасности программно-технических средств (ПТС) КЦОИ и автоматизированных систем (АС), функционирующих на КЦОИ БР, путем мониторинга и управления как специальными, так и встроенными в общесистемное программное обеспечение средствами обеспечения информационной безопасности (ИБ).

Цели создания СОИБ КЦОИ БР

Перед СОИБ КЦОИ БР стояли три основные цели:

1) выполнение в КЦОИ БР требований нормативных документов Банка России и стандарта Банка России по ИБ;
2) проведение централизованного управления учетными записями и правами доступа персонала СОИБ КЦОИ БР и подконтрольных СОИБ КЦОИ БР объектов;
3) обеспечение централизованного мониторинга и осуществление контроля выполнения персоналом СОИБ КЦОИ БР и подконтрольных СОИБ КЦОИ БР объектов регламентов и технологических операций.

Функции СОИБ КЦОИ БР

В рамках СОИБ КЦОИ БР выполняются такие функции, как управление учетными записями эксплуатационного персонала КЦОИ БР, централизованная аутентификация и управление доступом к ресурсам комплекса технических средств (КТС) КЦОИ БР, централизованный мониторинг, самоконтроль СОИБ КЦОИ БР, а также резервирование, хранение и восстановление данных СОИБ КЦОИ БР.

Структура СОИБ КЦОИ БР

Структурно СОИБ КЦОИ БР состоит из ядра системы и специализированных подсистем управления и мониторинга (СПУМ) в составе: СПУМ z/OS, СПУМ MS Windows КЦОИ БР, СПУМ ЛВС КЦОИ БР, СПУМ антивирусной защитой КЦОИ БР, СПУМ СЗИ от НСД и СПУМ СУБД КЦОИ БР.

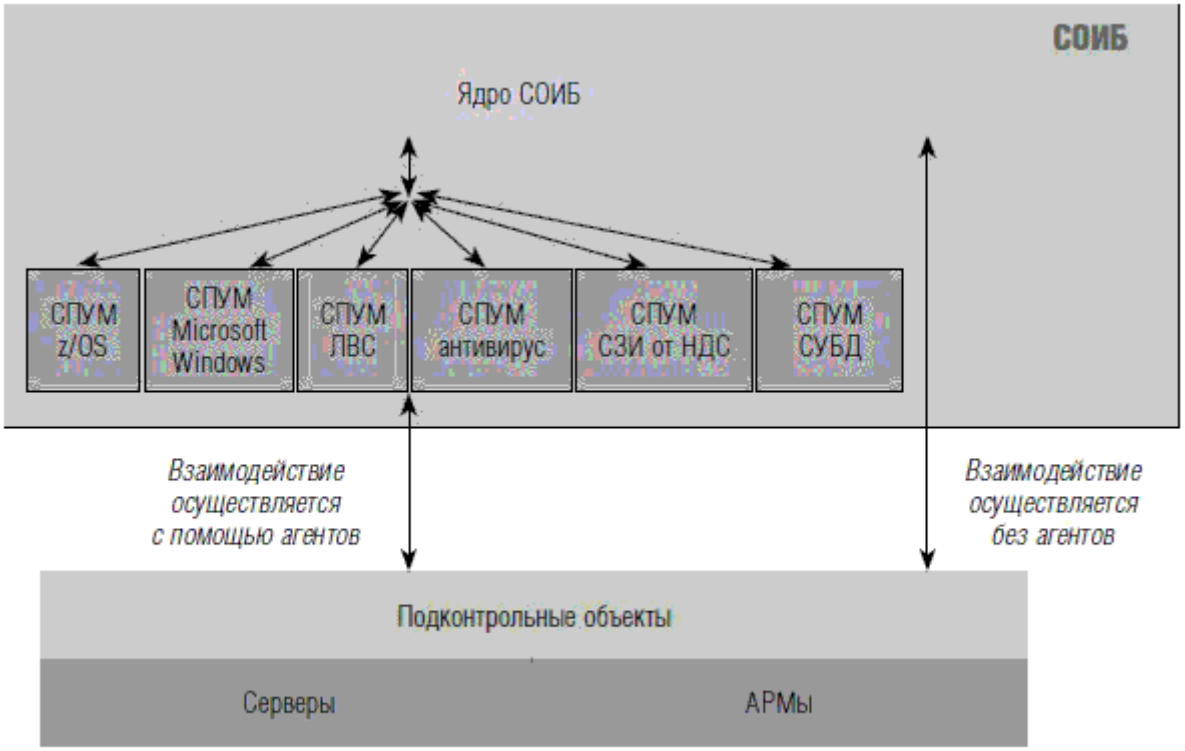


Рис. 8. Структура СОИБ КЦОИ БР

СОИБ КЦОИ БР обеспечивает реализацию требований к функциям СОИБ и взаимодействие со смежными специализированными подсистемами управления и мониторинга.

Ядро системы СОИБ КЦОИ БР обеспечивает выполнение функций СОИБ КЦОИ БР и осуществляет взаимодействие со СПУМ.

Специализированные подсистемы управления и мониторинга (СПУМ) СОИБ КЦОИ БР входят в состав СОИБ БР и обеспечивают взаимодействие ядра СОИБ БР с соответствующими подконтрольными системами КЦОИ БР.

Выполнение функций СОИБ КЦОИ БР в отношении подконтрольных объектов обеспечивается ядром СОИБ КЦОИ БР при отсутствии агентов на подконтрольных объектах или ядром СОИБ КЦОИ БР совместно со СПУМ при наличии агентов на подконтрольных объектах.

С целью обеспечения отказоустойчивости и катастрофоустойчивости работы СОИБ КЦОИ БР программные средства, обеспечивающие функционирование СОИБ КЦОИ БР, установлены особым образом, в специальной конфигурации и со специальными настройками.

Структурная схема

Структурная схема СОИБ КЦОИ представлена ниже. На схеме выделены объекты, подконтрольные СОИБ КЦОИ БР.

Программные средства подконтрольных систем состоят из операционных систем z/OS, Suse Linux и Windows Server 2003, Windows XP, WebSphere Application Server, СУБД Oracle и MS SQL.

Заключение

Следует отметить, что СОИБ КЦОИ БР является гибкой и развивающейся информационной системой. Продуманные особенности структуры СОИБ КЦОИ БР (ядро и набор СПУМ), а также мощность программных средств, используемых для реализации

системы, позволяют обеспечить широкие возможности по масштабируемости системы и добавлению новых подконтрольных систем в контур СОИБ КЦОИ БР в будущем.

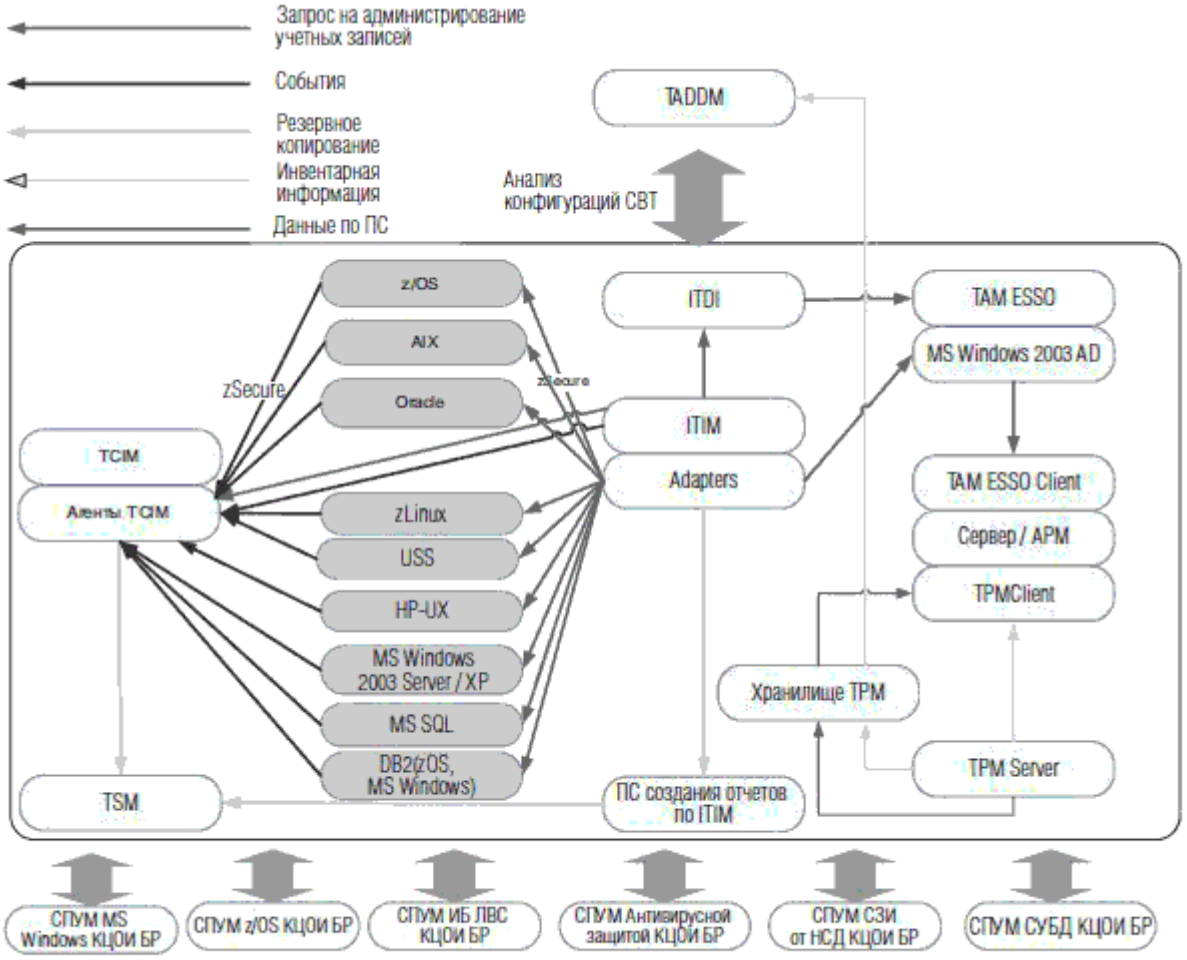


Рис. 9. Схема информационного взаимодействия

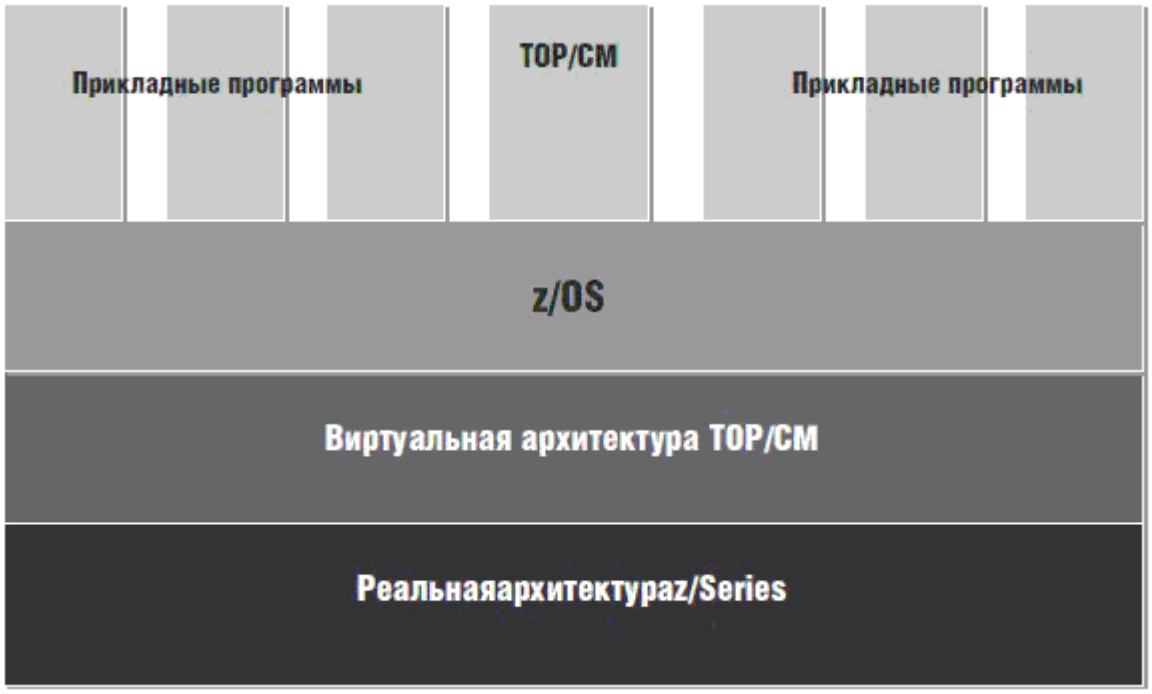
Приложение 5
Монитор TopCM

В ЗАО «ЕС-лизинг» разработан монитор TopCM (Top Control Manager), предназначенный для осуществления полного контроля над функционированием операционной системы z/OS вместе со всеми ее приложениями с целью обеспечения повышенного уровня информационной безопасности вычислительного процесса, построенного на базе z/OS. Монитор TopCM способен полностью контролировать взаимодействие вычислительной системы с внешней средой, включая взаимодействия с другими вычислительными системами посредством каналов связей, а также работу пользователей любого статуса, в том числе операторов и администраторов операционной системы и любых приложений. Кроме того, монитор может контролировать функционирование всех прикладных и системных программ, включая их взаимодействие друг с другом, попытки получения несанкционированного доступа к ресурсам, попытки неавторизованных программ нарушить или вмешаться в работу управляющей или других прикладных программ, а также повысить свой собственный статус или уровень авторизации в системе.

Одной из важнейших функций монитора является возможность обнаружения и пресечения попыток выполнения инструкций процессора, необъявленных в открытом описании принципов работы z/архитектуры. Возможность контролировать подобные события относится к программам любого типа, управляющим или прикладным, независимо

от уровня их авторизации.

Монитор TopCM запускается в среде z/OS как обычное задание в области V = R и представляет собой авторизованную программу. На этапе инициализации программа переходит в супервизорный режим и получает нулевой ключ доступа к памяти. Затем программа формирует свою собственную префиксную страницу и заменяет ею префиксную страницу z/OS. Если конфигурация вычислительной установки мультипроцессорная, TopCM заменяет своими собственными префиксные страницы z/OS для всех процессоров, входящих в конфигурацию.



Список литературы

1. Risk Metrics Technical Document. – JPMorgan, 4th edition, December, 1996
2. Taylor W. F. Principles of Scientific Management. – New York: Harper & Row, 1911.
3. Гольдштейн Г. Я. Основы менеджмента – Таганрог: ТРТУ, 2003.
4. ГОСТ Р 51897-2002, Менеджмент риска. Термины и определения.
5. ГОСТ Р 51898-2002, Аспекты безопасности. Правила включения в стандарты.
6. Нив Генри Р. Пространство доктора Деминга: Принципы построения устойчивого бизнеса. – М.: Альпина Бизнес Букс, 2005.
7. Deming W. Edward. Out of the Crisis: Quality, Productivity, and Competitive Position. – Cambridge (Mass.) Mass. Inst. of Technology, Center for Advanced Engineering Study: Cambridge University Press, 1982.
8. ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, 13 May 2004.
9. Европейское качество = European Quality: журнал/Европейская организация по качеству; перевод/ФГУП РИА «Стандарты и качество» – 2001, № 2.
10. ИСО 31000, Risk management – Principles and guidelines on implementation.
11. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
12. ISO/IEC 38500:2008, Corporate governance of information technology.
13. ISO GUIDE 72:2001, Guidelines for the justification and development of management system standards.
14. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance.

15. Technical Report ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.

16. NIST Special Publication 800-61, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, January 2004.

17. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

18. ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management.

19. Excerpted from the Executive Summary of the Report Issued by The Committee of Sponsoring Organizations of the Treadway Commission. «Internal control – Integrated framework», 1992.

20. The Committee of Sponsoring Organizations of the Treadway Commission. «Internal Control over Financial Reporting – Guidance for Smaller Public Companies», 2006.

21. ISO/ШС 20000, Information technology – Service management.

22. ISO/IEC 15939, Software engineering – Software measurement process.

23. ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement.

24. Gartner. The Price of Information Security. Strategic Analysis Report.

25. Курило А. П., Зефиров С. Л., Голованов В. Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006.

26. СТО БР ИББС – 1.0-2008 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

27. СТО БР ИББС – 1.1-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности.

28. BSI PAS 56 Guide to Business Continuity Management (BCM)

29. ISO/IEC 15504 Information technology – Process assessment.

30. NIST Special Publication 800-55 «Security Metrics Guide for Information Technology Systems.

31. Зефиров С. Л., Голованов В. Б. Как измерить информационную безопасность организации? Объективно о субъективном // Защита информации. Инсайд. 2006. № 3.

32. Risk Based Internal Auditing [Электронный ресурс]/The Institute of Internal Auditors – UK and Ireland. – www.iia.org.uk, August 2003.

33. К. В. Харский. Благонадежность и лояльность персонала. – СПб.: Питер,
2003.

34.. Robert H. Anderson, Richard Brackney, Thomas Bozek. Advanced Network Defense Research, Proceedings of a Workshop., Santa Monica, CA, RAND Corporation, CF-159-NSA, 2000.

35. Инструкция Банка России № 110-И «Об обязательных нормативах банков» от 16 января 2004 г.

36. DoD Insider Threat Mitigation. Final Report of the Insider Threat Integrated Process Team, 24.04.2000.

37. Marisa Reddy Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, Andrew Moore. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, National Threat Assessment Center, United States Secret Service, Washington, DC. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, August 2004.

38. «Сисадмин осужден на 8 лет за месть работодателю», http://forum.ubuntu.ru, 18.12.2006 г.

39. «Сисадмин банка уничтожил данные из-за маленькой премии», http://forum.armkb.com, 13.06.2006 г.

40. «Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing «Logic Bomb» on Company Computers», U. S. Department of Justice United States Attorney District of

New Jersey, December 17, 2002.

41 С. Витковская, А. Никольский ««Шерлок» взят с поличным. Бывшие сотрудники «ВымпелКома» продавали распечатки звонков сотовых абонентов», http://www.sostav.ru, 29.11.2004 г.

42. «Защита от инсайдера», приложение к газете «Коммерсантъ» № 69 (3645) от 24.04.2007 г. (http://www.kommersant.ru).

43. Дайджест событий ИТ-безопасности// КомпьютерПресс. 2007. № 5.

44. «Huge Leak Revealed at Japanese Firm», http://www.darkreading.com, 2007 г.

45. О. Визнюк «Запорожский хакер взломал банковскую систему», Центр исследований компьютерной преступности, http://www.crime-research.ru, 11.04.2005.

46. «Хакер сознательно хотел, чтобы его заметили, но этого не произошло», http://www.securitylab.ru, 12.04.2005.

47. «Жером Кервьель лишил главу Societe Generale половины полномочий», газета «Коммерсантъ», № 67 (3884) от 19.04.2008 (http://www.kommersant.ru).

48. «Societe Generale обнаружил дефекты в управлении рисками», газета «Коммерсантъ», № 30 (3847) от 22.02.2008 (http://www.kommersant.ru).

49. «У Жерома Кервьеля был шанс обыграть рынок» (http://bankir.ru, 25.12.2008).

50. «Жером-разоритель», журнал «Власть», № 4 (757) от 04.02.2008 (http://www.kommersant.ru).

51. Yann Le Guernigou, Tim Hepher. SocGen splits chairman, CEO jobs after scandal. – Reuters, 17.04.2008.

52. Скляров С. В. Вина и мотивы преступного поведения. – М.: Юридический центр Пресс, 2004.

53. Комер М. Дж. Расследование корпоративного мошенничества. – М.: Hippo, 2004.

54. Доронин А. И. Бизнес-разведка. – М.: Ось-89, 2003.

55. Report to the Nation on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, Inc., 2008.

56. Положение Центрального банка Российской Федерации от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».

Участники проекта «Обеспечение информационной безопасности бизнеса»

IBM Восточная Европа/Азия
123317, Россия, Москва,
Пресненская наб., д. 10
Тел.: +7 (495) 775-8800
Факс: +7 (495) 940-2070,
+ 7 (495) 258-6363
ibm.com/ru

CompuTel
115114, Россия, Москва,
Кожевнический пр., д. 4, стр. 3
Тел.: +7 (495) 640-3010
Факс: +7 (495) 640-3011
www.computel.ru info@computel.ru

ЗАО «ЕС-лизинг»
117405, Россия, Москва,

Варшавское ш., д. 125, стр. 1
Тел.: +7 (495) 319-1390
Факс: +7 (495)-319 6990
www.ec-leasing.ru contact@ec-leasing.ru

ЗАО НИП «ИНФОРМЗАЩИТА»
127018, Россия, Москва,
ул. Образцова, д. 38
Тел./факс: +7 (495) 980-2345
www.infosec.ru
Запрос информации о продуктах и услугах:
market@infosec.ru

ЗАО «Инфосистемы Джет»
127015, Россия, Москва,
ул. Б. Новодмитровская, д. 14, стр. 1,
офисный центр «Новодмитровский»
Тел.: +7 (495) 411-7601,
+ 7 (495) 411-7603
Факс: +7 (495) 411-7602
http://www.jet.msk.su info@jet.msk.su

ОАО «ЭЛВИС-ПЛЮС»
124498, Россия, Москва,
Зеленоград, Проезд 4806, д. 5, стр. 23
Тел.: +7 (495) 777-4290,
+ 7 (499) 731-4633,
+ 7 (499) 731-2403
www.elvis.ru
info@elvis.ru