Министерство образования и науки Республики Казахстан
Каспийский государственный университет технологий и инжиниринга имени Ш.Есенова

Ахметов Б.Б., Корченко А.Г., Архипов А.Е., Казмирчук С.В.

ПОСТРОЕНИЕ СИСТЕМ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ТЕОРИЯ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ (КНИГА 1)

Рекомендовано Ученым советом университета

Актау, 2018

УДК 004.056(02)
ББК 32.973.26-018.я73
П 63

Рецензенты:

Муратбеков М.М. – к.ф.-м.н., PhD, директор Центра информационных технологий Казахского университета экономики, финансов и международной торговли.

Жумабаева Л.О. – доцент кафедры «Компьютерный инжиниринг» Каспийского государственного университета технологий и инжиниринга им. Ш. Есенова.

Рекомендовано к печати Ученым советом Каспийского государственного университета технологий и инжиниринга имени Ш.Есенова.

П 63 Б.Б. Ахметов, А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. Построение систем анализа и оценивания рисков информационной безопасности. Теория и практические решения. Монография. В 2-кн. Кн. 1, Актау: редакционно-издательский отдел КГУТИ им.Ш.Есенова, 2018 – 387 с., 33 пл.

ISBN 978-601-308-081-9

Монография посвящена теоретико-методологическим и практическим аспектам оценивания рисков информационной безопасности. Рассмотрены базовые понятия и модели рисков, международные и национальные нормативные документы в сфере оценивания и управления рисками. Значительное внимание уделено оцениванию потерь, обусловленных реализацией угроз информации (модели потерь, шкалы и структуры ценности информационных ресурсов, нониусная и сценарная методики определения потерь), и вероятностных параметров рисков. Уделено внимание разработке методов модификации порядка лингвистической переменной при переопределении эталонов параметров, а также оцениванию рисков безопасности ресурсов информационных систем в реальном времени с использованием CVSS метрик, которые содержатся в открытых базах данных уязвимостей. Подробно рассмотрены вопросы практического оценивания рисков без привлечения экспертов соответствующей предметной области при нечетких и детерминированных условиях оценивания с использованием параметров, которые могут быть представлены как в числовой, так и лингвистической форме с учетом периода времени, отрасли промышленности, экономической и управленческой специфики предприятия.

Книга предназначена для научных работников, инженеров, аспирантов и студентов высших учебных заведений соответствующего профиля.

ISBN 978-601-308-081-9

УДК 004.056(02)
ББК 32.973.26-018.я73

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ СОКРАЩЕНИЙ

АИС	автоматизированная информационная система
АОР	анализ и оценивание рисков
АС	автоматизированная система
АСУ	автоматизированная система управления
АТС	автоматическая телефонная станция
АЭС	атомная эклетро станция
БД	базы данных
БДУБИ	банк данных угроз безопасности информации
ВВ	вероятностями возникновения
ВКК	величина капитала компании
ВСИ	вероятность сценария инцидента
ДТП	дорожно-транспортные происшествия
ЕСО	эмпирическая система с отношением
ЗИ	защита информации
ИА	информационные активы
ИБ	информационная безопасность
ИКС	информационно-коммуникационные системы
ИР	информационные ресурсы
ИС	информационная система
ИсОД	информация с ограниченным доступом
ИТ	информационные технологии
ИТС	информационно-телекоммуникационная система
ИТТ	информационно-телекоммуникационные технологии
КД	корпоративные данные
КЛ	количественная
КСЗИ	комплексная система защиты информации
КЧ	качественная
ЛПР	лицами, принимающими решения
МАИ	метод анализа иерархий
МБК	модуль бинарной классификации
МБС	метод на основе байесовских сетей
МГ	метрическая группа
МНСИ	материальный носитель секретной информации
МР	мера риска
НМД	несанкционированная модификация данных

МОЭ	многообъектная экспертиза
НСБ	непредвиденная ситуация в бизнесе
НСД	несанкционированный доступ
НСМ	несанкционированная модификация
НТП	научно-технический прогресс
ОИД	объект информационной деятельности
ОПД	объект предпринимательской деятельности
ОР	объекты риска
ОР	оценка рисков
ОС	операционная система
ОУ	оценка угрозы
ПВР	показатель вероятности риска
ПК	персональный компьютер
ПО	программное обеспечение
ПС	программное средство
РИС	ресурсы информационной системы
РОП	риск-ориентированный подход
РП	рискообразующий потенциал
РС	рисковую ситуацию
СВР	степень возможности реализации угроз
СЗИ	средства защиты информации
СИ	секретной информации
СМБИ	система менеджмента безопасности информации
СМЗИ	система менеджмента защиты информации
СМИБ	система менеджмента информационной безопасности
СОБ	субъекты обеспечения безопасности
ССГТ	Свода сведений, составляющих государственную тайну Украины
СТП	степень тяжести последствий от потери
СУБД	система управления базами данных
СЧО	составная часть объекта
ТВ	тематический вопросник
ТП	технологические процессы
УБИ	угроза безопасности информации
УР	уровень риска
ЦА	ценность актива
ЦО	целевые объекты

ЧСО	числовая система с отношениями
ЭК	экспертная комиссия
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
ISO	Международная организация по стандартизации
IEC	Международная электротехническая комиссия
NVD	National Vulnerability Database
OSVDB	Open Sourced Vulnerability Database
SCAP	Security Content Automation Protocol

ВВЕДЕНИЕ

Стремительное развитие IT-инфраструктуры предприятий неизменно влечет за собой неконтролируемый рост количества угроз и уязвимостей информационных ресурсов (ИР). В этих условиях оценивание информационных рисков позволяет определить необходимый уровень защиты информации (ЗИ), осуществить его поддержку и разработать стратегию развития информационной структуры объекта защиты. Анализ и оценивание рисков (АОР) является необходимым условием при создании системы управления рисками [1] и плана работ по обеспечению информационной безопасности (ИБ).

Согласно требованиям Закона Украины «О защите информации в информационно-телекоммуникационных системах» для обеспечения безопасности ИР, обрабатываемых в автоматизированной системе (АС), необходимо разрабатывать комплексную систему защиты информации (КСЗИ). Базовым этапом ее построения, является создание политики безопасности [2], методология которой включает в себя:

- разработку концепции ИБ в АС;
- анализ рисков;
- определение требований к мерам, методам и средствам защиты;
- выбор основных решений по обеспечению ИБ;
- организацию выполнения восстановительных работ и обеспечение непрерывного функционирования АС;
- документальное оформление политики безопасности.

В свою очередь для анализа рисков необходимо:

- определить базовые составляющие АС и составить реестр ее ресурсов, которые учитываются при анализе;
- идентифицировать угрозы объектам защиты;
- оценить риски и величину возможных убытков, связанных с реализацией угроз;
- определить варианты и затраты на построение КСЗИ [3].

На сегодняшний день существует множество средств, используемых для АОР, которые представлены в достаточно широком спектре, начинающемся нормативными документами (стандартами) и

заканчивающемся конкретными программными приложениями. При выборе последних для их использования в практической деятельности эксперт сталкивается с множеством вопросов, например: «Какие использовать параметры?», «Какой математический аппарат применять в ходе проведения АОР?», «Как оценить параметры рисков при отсутствии статистических данных?», «Как произвести АОР в условиях нечеткости?» и т.д. Эти и другие факторы создают ряд трудностей при выборе соответствующих средств оценивания. Следует отметить, что в основном для АОР предполагается использование статистических данных об инцидентах и угрозах ИБ. Однако во многих странах (в том числе и в Украине) нет соответствующей государственной политики относительно регистрации и применения подобной статистики [4], что ограничивает возможности применения существующих методик и инструментальных средств для выполнения АОР. Еще одним фактором, который усложняет эксперту возможность использования при АОР более широкого спектра параметров, является наличие определенных ограничений (на используемый набор параметров) в подобных средствах, что в свою очередь понижает их гибкость.

Глава 1. БАЗОВЫЕ ПОНЯТИЯ И СОВРЕМЕННОЕ СОСТОЯНИЕ В ОБЛАСТИ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Исследование понятия риска

Часто перед специалистами компаний для повышения эффективности решения задач ЗИ возникает вопрос о выборе соответствующей методики, которая будет удовлетворять адекватным требованиям. Прежде чем осуществлять такой выбор необходимо иметь достаточно полное отображение понятия риска в аспекте ИБ. В различных публикациях существует множество определений риска [5-52], несущих достаточно широкое его трактование. Только в Интернет-словарях содержится свыше 1500 толкований риска во многих сферах человеческой деятельности [15]. Вследствие этого возникают различные неоднозначности, связанные с раскрытием сущности самого риска и связанных с ним понятий. Соответственно такое состояние характерно и для сферы ИБ. В этой связи, анализ и раскрытие понятия риска, для его последующий интерпретации в области ИБ, расширит возможности по повышению эффективности решений задач ЗИ. Учитывая, что риски затрагивают различные предметные области, то это понятие следует рассмотреть с точки зрения безопасности, психологии, экономики, страхования, медицины, геологии и т.д., которое раскрывается как в монографиях, статьях, учебниках, словарях так и различных нормативных, национальных и международных документах.

В большинстве указанных источников риск часто отображается вероятностью или связанными с ней понятиями, например как, **измеряемая или рассчитываемая вероятность:**

- потерь [15, 31, 49];
- появления неблагоприятного исхода [31, 42] или события, например, в результате которого возможны непредвиденные потери [17, 40];
- возможности опасности, неудачи [24], получения результата от принимаемого решения [15, 31], не достижения цели [15], появления обстоятельств обусловливающих неуверенность или невозможность получения ожидаемых результатов от реализации поставленной цели [35];

− понести убытки или упустить выгоду (количественно измеряемая неуверенность в получении соответствующего дохода или убытка) [35, 37];

− реализации определенной угрозы, вида и величины нанесенного ущерба [10, 31, 38, 45];

− причинения вреда имуществу, окружающей среде или жизни (здоровью) граждан, животных, растений [36];

− возникновения заданной угрозы и потенциально неблагоприятных последствий возникновения этой угрозы [14];

− подразумевающую потенциальную возможность нарушения безопасности [18];

− данной угрозы, с помощью которой будут использоваться уязвимости актива или группы активов, чтобы привести к потере и/или повреждению имущества [41];

− сочетание или комбинация вероятности события и его последствий [12, 21, 27, 33, 40, 43, 46].

Известно, что вероятность связанна с наступлением определенного события [14, 19, 32], а соответственно с ним здесь связан и риск, что также видно из выше проведенного анализа публикаций.

Так же в литературе встречается определение риска как **действие или деятельность:**

− реализация которого ставит под угрозу удовлетворение какой-либо достаточно важной потребности [34];

− состоящая в неопределенности ее исхода и возможных неблагоприятных последствиях в случае неуспеха для субъекта [16, 23];

− в том, или ином отношении грозящее субъекту потерей (проигрышем, травмой, ущербом) [23, 25];

− в условиях неопределенности и деятельность субъекта, связанная с преодолением неопределённости [15];

− наудачу в надежде на счастливый исход [24].

Как известно **действие или деятельность** [14], также, как и **вероятность** (измеряемая или рассчитываемая) связаны с возникновениями каких-либо характерных для них событий. Также известно, что любые действия приводят к событиям и последствиям, которые могут представлять собой как потенциальные «положитель-

ные» возможности, так и «опасности» [15]. Исходя из сказанного, в этом контексте прослеживается общность указанных понятий.

В отдельных источниках риск трактуется как **мера:**

− ожидаемого неблагополучия при неуспехе в деятельности, определяемая сочетанием вероятности неуспеха и степени неблагоприятных последствий в этом случае [23];

− неопределенности и конфликтности в предпринимательской деятельности [15];

− различия между разными возможными результатами принятия определенных стратегий (решениями задачи) [19];

− опасности, характеризующая вероятность ее появления и размеры связанного с ней ущерба [28, 30];

− возможности реализации опасности в виде определенного ущерба в искусственно созданной действиями субъекта ситуации [9];

− возникновения в любой системе нежелательного события с определенными во времени и пространстве последствиями [29].

Здесь видно, что трактование риска также связано с наступлением определенного события, а мера выступает в качестве вторичного фактора и непосредственно связана с количественным или качественным оцениванием.

Следует заметить, что в аналогичном качестве мера имеет место и для **измеряемой или рассчитываемой вероятности,** а также **действия или деятельности.** Мера обычно интерпретируется количественными и качественными показателями, а так же их сочетанием. С философской точки зрения [8, 50] мера рассматривается как взаимосвязь и взаимозависимость количественных и качественных изменений, а в метрологии [14], как средство измерения, предназначенное для воспроизведения и хранения физической величины. Поэтому интерпретация понятия меры относительно определения риска направлена на его отображение (в чем он измеряется) в сочетании «мера риска». Риск связан также с неопределенностью, необходимостью субъекта использовать аналитические методы и интуицию, а также возможностью получения как положительных, так и отрицательных результатов [15].

Риск определяется как **неопределенность**:

− например, предполагающая возможность ущерба состояния защищенности интересов (целей) организации банковской системы страны в условиях угроз в информационной сфере [39];

− в аспекте контроля и прогноза будущего человеческой деятельности [44].

Встречаются и определения риска, которые отображают его как опасность, ситуацию выбора из двух или **n** вариантов действия.

Как **опасность**:

− предполагаемая (известная);

− неизвестная на данный момент, но которая может появиться [5, 37];

− нанесения ущерба посредством атаки (реализации некоторой угрозы с использованием уязвимости актива или группы активов [12]).

Ситуация выбора из двух или из **n** вариантов действия (поведения):

− связанного с возможной неудачей, с одной стороны, и предполагающего хотя бы минимальное сохранение уже достигнутого, с другой [34];

− менее привлекательным (однако более надежным) и более привлекательным, (менее надежным, исход которого проблематичен и связан с возможными неблагоприятными последствиями) [23].

Здесь также видно, что рассмотренные понятия риска, которые трактуются как **опасность** (возможность появления какого-либо нежелательного события [32]), **ситуация выбора** из двух или из **n** вариантов действия (поведения) и неопределенность, как и в предыдущих случаях, связаны с наступлением в какой-то **мере** определенного события. Известны понятия риска, которые определяют его как частоту, величину, характеристику ситуации и т.д., которые напрямую связаны с возникновением того или иного события.

Приведем некоторые из них, например, риск как:

− **частота** реализации «опасности» [20];

− произведение величины события на меру ее возможности [22];

− **характеристика ситуации**, с неопределенностью исхода, при наличии неблагоприятных последствий; предположение

неуверенности (невозможности получения достоверного знания) о благоприятном исходе в заданных обстоятельствах [31, 51];

− **событие**, которое может произойти или не произойти [15] или ожидание её наступления (потенциально нежелательных воздействий на актив или его характеристики, которые могут быть следствием некоторого прошлого, настоящего или будущего события [6, 31]);

− **затраты или потери** экономического эффекта, связанные с реализацией определенного решения (например, планового варианта) в условиях, иных по сравнению с теми, при которых решение было бы оптимальным [16, 52].

Также риск в любом контексте рассматривается как суммарная величина угрозы (то есть события, которые наносят ущерб), уязвимости (открытость предприятия к угрозам) и стоимости имущества (стоимость актива при опасности) [47, 53, 54, 55].

Сущность риска и его свойства

В повседневном общеупотребительном применении термин «риск» имеет два достаточно отличающихся смысла. Так, по словарю Ожегова [24] в своем первом значении риск – это возможная опасность, и связанное с нею ожидание возможных потерь, неудач, негативного развития событий и тому подобное. Вторая трактовка словарем этого термина: действие наудачу в надежде на счастливый исход. Как видим, эта трактовка шире первой, добавлен позитив – надежда на лучшее развитие событий, хорошие результаты их развития, удачно принятые решения. То есть по второй трактовке риск – это еще и поиск успешных альтернатив в противостоянии опасностям и невзгодам в условиях неопределенности и необходимости/неизбежности выбора, преодоление негатива, возможного в этих ситуациях. В этом смысле термин «риск» достаточно близок пониманию содержания этого понятия в толковом словаре украинского языка [56], в котором риск, рискованное действие определяется как:

1. Осознанная возможность опасности, смелый, инициативный поступок, действие в надежде на счастливый исход, успех, позитивный результат.

2. Возможность возникновения потерь, убытков или неудачи в каком-то деле.

Общеизвестно, что категориально понятийный аппарат составляет фундамент любой проблемы и одновременно является инструментом ее исследования. В этом смысле ситуация с определением термина «риск» представляется крайне тяжелой. Покажем это, приведя несколько толкований данного термина.

1. «Риск – прогнозируемая векторная величина ущерба, который может возникнуть в результате принятия решений в условиях неопределенности и реализации угрозы. Он является количественной мерой безопасности, равной произведению вероятности реализации данной угрозы, умноженной на вероятность величины (величину) возможного ущерба от нее» [57].

2. «Риск – это вероятность того, что действия человека или их результаты приведут к негативным или позитивным последствиям» [58].

3. «Риск – количественная мера опасности с учетом ее последствий. Последствия проявления опасности всегда приводят к ущербу, который может быть экономическим, социальным, экологическим и т.д. Поэтому оценка риска должна быть связана с оценкой ущерба. Чем больше ожидаемый ущерб, тем выше риск. Кроме того, риск тем выше, чем больше вероятность проявления соответствующей опасности. Словом понятие «риск» объединяет два понятия – «вероятность опасности» и «ущерб» [59].

4. «Риск – возможность таких последствий принятия решений, при которых поставленные цели частично или полностью не достигаются. Такое толкование риска предполагает, что он возникает тогда, когда решения принимаются при наличии нескольких альтернатив» [60].

5. «Риск – это деятельность, связанная с преодолением неопределенности в ситуации неизбежного выбора, в процессе которой имеется возможность количественно и качественно оценить вероятность достижения допустимого результата, неудачи, или отклонения от цели» [61].

6. «Риск – это возможность отклонения фактических результатов деятельности (работы) от ожидаемых или нормативных значений» [62].

7. «Риск – вероятность возникновения убытков или недополучения доходов по сравнению с прогнозируемым вариантом» [63].

8. «Риск – вероятность причинения вреда с учетом его тяжести» [64].

Приведенные выше определения очевидно свидетельствуют об отсутствии единого однозначного понимания термина «риск». Это неудивительно, потому что, как уже отмечалось во Введении, риски объективно присутствуют практически во всех сферах деятельности людей, в их взаимоотношениях с окружающей средой. Соответственно в каждой из этих сфер риски имеют свои особенности, свои определенные специфические проявления, что и приводит к появлению большого количества отличных друг от друга определений понятия «риск».

Тем не менее, исследуя множество рисков, можно обнаружить в них наличие определенных общих черт. **В частности, глобальной общей чертой, характерной для всего множества рисков, является обязательное существование ситуации неопределенности, которая фактически и порождает риск.** Чтобы иметь возможность более основательно ознакомиться со свойствами рисков, определим содержание ряда категориальных понятий, непосредственно связанных с существованием и исследованием рисков. Введем три категориальных понятия.

Первое – **объекты риска (ОР)**. Это собственно человек и связанные с его существованием и деятельностью объекты из самых разных сфер: социальной, хозяйственной, экономической, политической и т.д., то есть это промышленные и сельскохозяйственные предприятия, торгово-экономические, медицинские, культурно-развлекательные организации и учреждения, государственные учреждения, политические партии, международные организации и т.п. Принципиально важным в определении ОР является выявление цели (смысла, миссии) его существования (деятельности, функционирования) и индикатора (показателя) состояния ОР, причем для более или менее сложных объектов эти две характеристики ОР могут быть комплексными, иметь векторный характер. Важным также является очевидная зависимость качества функционирования ОР, в смысле степени (меры) успешности достижения цели его

функционирования, от состояния ОР. Это определяется двумя обстоятельствами:

− часто существующей на практике невозможностью непосредственного контроля качества функционирования ОР, в связи с чем степень достижения цели функционирования ОР оценивается опосредствованно через контролируемые значения параметров текущего состояния ОР;

− насущной потребностью в прогнозе степени реализации целей функционирования ОР в будущем через известные значения параметров его текущего состояния и ряда предыдущих значений этих параметров.

Следующей категорией являеися **ситуация неопределенности** – совокупность обстоятельств и условий, при которых вероятные изменения состояния ОР становятся совершенно непредсказуемыми. Эта ситуация исключает возможность объективного оценивания риска. Некоторое снижение неопределенности до уровня так называемой статистической неопределенности порождает еще одно категориальное понятие – **рисковую ситуацию** (РС), которая характеризуется существованием нескольких возможных состояний ОР (как вариант – множества состояний, достигает бесконечности), вероятность реализации каждого из которых известна. Если реализацию на ОР любого из возможных состояний считать событием, **РС определяется существованием множества вариантов возможного развития событий, вероятность каждого из которых характеризуется соответствующей количественной или качественной оценке.** В условиях возникновения рисковой ситуации становится актуальным проведение анализа и оценки рисков, в том числе исследования обстоятельств появления, условий и форм развития рисков.

Понятийный аппарат, механизм возникновения и развития рисков

Для значительной группы реальных рисков образования рисковой ситуации является следствием воздействия опасностей различного происхождения на ОР. В рамках этой гипотезы считается, что результатом реализации опасностей является совокупность возможных негативных событий, каждое из которых характеризуется

вероятностью своей реализации и определенными последствиями, которые могут возникнуть в случае реализации этого события. Обязательным условием порождения риска является наличие нескольких вариантов возможного развития негативных событий, то есть неопределенность на уровне реализации опасностей, в том числе порожденных ими угрожающих явлений и процессов, которые негативно влияют на функционирование ОР. Приведенная схема хорошо соотносится с механизмом образования рисков в процессе взаимодействия человека с природой, техносферой, в частности актуальна для задач защиты информации.

Чтобы иметь возможность более основательно ознакомиться со свойствами этого механизма, определим содержание ряда понятий, непосредственно связанных с исследованием ситуации «опасность-риск». Первое из них – это **опасность**. В общем случае **опасность** – это свойство среды функционирования ОР, которое заключается в возможности порождения этой средой негативных воздействий на ОР и его окружения. Воздействие опасности на ОР осуществляется через **источники опасности**, которыми являются природные процессы и явления, техногенные воздействия, человеческая деятельность, в общем, все то, что способствует возникновению и реализации опасностей в любой форме.

Существуют многочисленные классификации опасностей [58]. Например, по источнику возникновения выделяют пять групп опасностей: природные, техногенные, социальные, экономические, политические; по масштабам последствий – бытовые, локальные, региональные, глобальные; по важности (тяжести) последствий – инцидент, событие, авария, катастрофа. Исходя из требований обеспечения постоянной жизнедеятельности людей, существования и развития промышленных социальных систем, выделяют два вида опасностей: опасности деятельности и опасности территории. Первый тип связан со свойством определенных видов деятельности порождать (формировать) источники опасностей техногенного, социального, экономического или политического характера, второй – существованием подобных источников и источников природного происхождения в пределах определенной территории или рядом с ней.

Следует отметить, что человеческая деятельность, как активное и сознательное взаимодействие человека со средой обитания, является атрибутом цивилизационного процесса, она всегда и везде сопровождает человека. С другой стороны, жизненный опыт человечества показывает, что любой вид деятельности, будучи полезным для его существования, одновременно может быть источником негативных воздействий, то есть потенциальная опасность является универсальным свойством процесса взаимодействия человека со средой обитания на всех стадиях жизненного цикла как в быту, так и в социально-производственной сфере. Полученный вывод называют аксиомой о потенциальной опасности деятельности, который имеет два последствия, важных для формирования систем безопасности:

− ни один вид деятельности не может обеспечить абсолютную безопасность для человека;

− невозможно разработать абсолютно безопасную технологию или технику.

Учитывая глобальный характер человеческой деятельности, можно считать, что «чистая» **опасность территории** определяется только существованием источников опасностей природного происхождения, все другие источники своим существованием обязаны человеку.

В зависимости от локализации опасностей во времени, их продолжительности, повторяемости выделяют:

− **опасные явления** – эпизодически возникающие опасности, имеют короткий срок существования;

− **опасные процессы** – продолжительные и распределенные во времени опасности;

− **потоки опасных событий (явлений)** – последовательности случайно распределенных во времени опасных явлений.

Конкретизация форм непосредственного воздействия опасности на ОР приводит к выделению так называемых **рискообразующих (опасных) факторов**, воздействие которых на ОР может нанести ему вред, стать причиной возникновения потерь, убытков, т.е. создает **угрозу** существованию и/или деятельности ОР. Очевидно, что возникновение угрозы становится возможным лишь при условии:

а) нахождения ОР в пределах воздействия на него опасности;

б) возможности поражения ОР вследствие действия рискообразующих факторов, порожденных влиянием опасных явлений или процессов.

Можно сказать, что наличие опасности является и свидетельством, и следствием объективного существования источников опасности, тогда как появление угрозы – уже существование возможности непосредственной реализации воздействия определенных негативных процессов или явлений на ОР. Причем мера этой возможности зависит не только от уровня действующих опасных воздействий (рискообразующих факторов угрозы), но и от наличия в ОР уязвимостей к данной угрозе (**уязвимость** – свойство ОР, заключается в его неспособности противостоять действию определенной угрозы или группы угроз). Следствием реализация угрозы становится нанесение **вреда** ОР. Если негативные последствия (то есть вред) допускают свою оценку в той или иной форме, имеют место **потери,** а потери, оцененные в денежно-стоимостной форме, составляют **убыток.**

Проиллюстрируем изложенный выше материал примером.

Для горной местности типичные опасности – опасности территории. Источники этих опасностей – природные явления и процессы, следствием реализации которых становится (в зависимости от времени года, метеорологических условий, особенностей местного климата и др.) формирования оползней, обвалов, селей, лавин. В случае их схода и при условии пребывания человека в зоне досягаемости действия этих явлений формируются непосредственные угрозы жизни людей, их здоровью и деятельности, угрозы разрушения или уничтожения поселений, отдельных сооружений, имущества. Поэтому только сам факт пребывания людей в горной местности в любом качестве (местного жителя, туриста, отдыхающего, наемного работника и т.п.) или осуществления там определенной деятельности уже составляет для них определенную опасность. Если в характеристики возникшей **опасной ситуации** включить количественные или качественные оценки вероятностей реализации опасных событий в пределах определенной территории, мы получаем типичную РС. Само описание этой РС будет содержать совокупность перечисленных выше опасных явлений (сокра-

щенная запись их наименований представлена четверкой $E = < e_1, e_2, e_3, e_4 >$, порядок элементов которой соответствует приведенному перечню природных явлений) и вектор $P=[p_1, p_2, p_3, \ldots]$ вероятностей реализации соответствующих угроз для ОР в данной местности. Количественные значения вероятностей иногда рассматривают как риски, интерпретируя последние как **меру опасности**, обусловленной возможностью реализации соответствующей угрозы, то есть в понятие «риск» вкладывается понятие меры возможности реализации опасности. Однако собственно оценки вероятностей являются очень общим показателем, который никак не учитывает последствий возможного влияния возникшей опасности на конкретного человека или другой ОР.

Более объективную информацию о реальной мере опасности можно получить, учитывая наряду с вероятностями реализаций возможных угроз и уровень вреда, причиненного ОР в результате воздействия на него этих угроз. При этом, анализируя вред, следует учитывать не только «прямой» ущерб (например, потери, нанесенные ОР в результате реализации угроз), но и другие возможные последствия, обусловленные полной или частичной утратой ОР качества своего функционирования вследствие реализации возможных угроз. Например, если ОР – метеорологическая станция, построенная в горной местности, и вероятность схода снежных лавин для места его непосредственного расположения равна $p_л$, то вред, который несет реализация этого события, имеет две составляющие:

$q_{пр}$ – стоимость полного или частичного (в зависимости от реально возможного уровня разрушения станции сходом лавины) восстановления поврежденного сооружения и оборудования метеостанции и

$q_{функ}$ – общая стоимость потерь, причиненных региону вследствие ошибок или неточностей региональных метеопрогнозов из-за отсутствия необходимой метеоинформации. Тогда произведение

$$r_л = p_л (q_{пр} + q_{функ})$$

определяет **уровень риска** (или просто **риск**), с которым сталкивается ОР в условиях возможного схода лавин. То есть в данном случае риск – это количественная мера опасности, исчисляемая как возможные убытки, причиненные сходом лавин.

Аналогичным образом можно вычислить риски ОР, которые возникают в случае возможной реализации любой из трех других приведенных выше угроз. При этом каждый отдельный (частный) риск r является показателем возможного вреда, который учитывает уровень неопределенности относительно возможности реализации соответствующей угрозы: чем выше вероятность ее реализации, тем ближе величина риска к своему максимальному значению, и наоборот, чем ниже вероятность реализации, тем меньше вероятный вред $r = pq$. Описание набора рисков, характерных для определенного ОР, образует **профиль рисков.**

Если предположить, что каждая из угроз может реализовываться только в одиночку, то сумма всех частных рисков (так называемый средний риск) будет представлять собой показатель уровня опасности, в котором интегрально учтены уровни неопределенности реализации каждой из угроз и соответствующие величины ущерба. Следует отметить, что описанная выше ситуация весьма упрощена, потому что в действительности рассмотрены угрозы не являются независимыми. В частности, реализация угрозы схода снежной лавины может сопровождаться другими угрозами (например, снежная масса лавины стимулирует реализацию обвала в непосредственной близости к ОР), поэтому оценка совокупного риска должна учитывать все возможные в этой ситуации сценарии реализации угроз.

Следует также отметить, что более тщательный анализ рассмотренной выше рисковой ситуации приводит к необходимости введения так называемых **динамических рисков**, то есть рисков, величина которых меняется во времени. В приведенном примере это объясняется тем, что значение вероятностных параметров схода снежной лавины или селя зависят от времени года, что вызывает изменения уровней соответствующих рисков во времени.

Для корректного формирования описательной схемы возникновения и вычисления рисков к приведенному выше необходимо добавить некоторые замечания.

Во-первых, ключевым условием образования рисковой ситуации является наличие неопределенности, которая обуславливается существованием множества вариантов возможного развития событий в результате реализации угроз ОР. Во-вторых, как уже отмечалось выше, должны быть известны вероятностные характеристики реализаций всех вариантов. В-третьих, определение среднего риска как суммы частных рисков (рисков каждого отдельного варианта развития событий) возможно только в случае, если математической моделью рисковой ситуации является полная группа событий [26], то есть когда для множества вариантов событий $\{e_i\}$, $i = \overline{1,n}$, выполняются условия:

$$\sum_{i=1}^{n} p_i = 1,$$

где p_i – вероятность реализации варианта v_i, и

$$p(v_i \cap v_j) = 0 \text{ при } i \neq j,$$

что является требованием попарной несовместности вариантов.

Поясним третье утверждение с помощью иллюстративного примера: предположим, что для ОР – здания, расположенного в горной местности, по особенностям его расположения актуальны две независимые угрозы – оползня thr_1 и обвала (камнепада) thr_2. Вероятности реализации этих событий – p_1 и p_2, последствия – соответствующие потери (убытки) q_1 и q_2. Необходимо рассчитать обобщающий (интегральный) показатель уровня опасности для ОР. Показателем, удовлетворяющем этому требованию, можно считать интегральный риск

$$R_{\text{int}} = P_d Q_d, \tag{1.1}$$

его можно трактовать как возможные интегральные потери Q_d, которые с вероятностью P_d претерпевает ОР при реализации опасности в любых ее проявлениях. Распространенной формой такого показателя, в том числе в финансово-экономической сфере [60-64],

считается так называемый суммарный риск R_Σ, представляющий собой сумму частных рисков, обусловленных возможностями реализации каждой из существующих угроз, актуальных для ОР, количество которых в общем случае равна n:

$$R_\Sigma = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i q_i. \qquad (1.2)$$

Для нашего примера $n = 2$, следовательно, по формуле (1.2) имеем: $R_\Sigma = p_1 q_1 + p_2 q_2$. Предположим, что $q_1 = q_2 = q$, тогда

$$R_\Sigma = (p_1 + p_2) q. \qquad (1.3)$$

Из сравнения формул (1.1) и (1.3), принимая во внимание цель введения показателя суммарного риска, следует ожидать выполнения условия:

$$P_d = p_1 + p_2. \qquad (1.4)$$

Для вероятности P_d очевидно неравенство $0 \le P_d \le 1$, соответственно для произвольной вероятности p_i – неравенство $0 \le p_i \le 1$, откуда для правой части условия (1.4) получаем соотношение $0 \le p_1 + p_2 \le 2$, которое позволяет утверждать, что равенство (1.4) не выполняется, то есть суммарный риск R_Σ не является показателем интегрального риска.

Из теории вероятностей известно, что вероятность P_d реализации опасности в любых ее проявлениях определяется для системы из двух независимых, но совместных угроз по формуле

$$P_d = p_1 + p_2 - p_1 p_2,$$

однако вопрос определения потерь Q_d в общем случае, когда $q_1 \ne q_2$, не является очевидным, а потому непосредственное применение формулы (1.1) для расчета интегрального риска представляется невозможным.

Чтобы справиться с этой проблемой, построим из независимых, но совместных угроз thr_1 и thr_2 множество независимых и несовместных событий, для которых можно достаточно просто рассчитать значения потерь (табл.1.1).

Таблица 1.1. Исходные данные для расчета интегрального риска

Варианты комбинированных угроз	Вероятности реализации комбинированных угроз	Потери от реализации комбинированных угроз	Частичные риски комбинированных угроз r_i
$E_1 = thr_1 * \overline{thr_2}$	$p_1(1-p_2)$	q_1	$q_1 p_1(1-p_2)$
$E_2 = \overline{thr_1} * thr_2$	$(1-p_1)p_2$	q_2	$q_2(1-p_1)p_2$
$E_3 = thr_1 * thr_2$	$p_1 p_2$	q_3	$q_3 p_1 p_2$
$E_4 = \overline{thr_1} * \overline{thr_2}$	$(1-p_1)(1-p_2)$	0	0

В табл. 1.1 идентификатором thr_i обозначено событие, заключающееся в реализации угрозы thr_i, а через $\overline{thr_i}$ – событие, являющееся дополнением к thr_i (то есть его отрицание). Из табл. 1.1 очевидно, что события (комбинации угроз) E_1 E_2, E_3, E_4 образуют полную группу, для элементов которой известны или вычислимы все параметры за исключением значения потерь q_3. По смыслу задачи эти потери, скорее всего, равны большему из значений q_1 или q_2, в частности, если известно, что $q_1 < q_2$, то $q_3 = q_2$.

Суммарный риск такой полной группы состоит из суммы частных рисков трех первых событий и равен интегральному риску:

$$R_{\text{int}} = R_{\Sigma} = q_1 p_1(1-p_2) + q_2 p_2 .$$

При известных значениях R_i и P_d из формулы (1.1) можно найти интегральные потери:

$$Q_d = [q_1 p_1(1-p_2) + q_2 p_2] / [p_1 + p_2 - p_1 p_2] .$$

Отметим, что при одновременной реализации угроз thr_1 и thr_2, если это не противоречит содержанию задачи, часто принимается гипотеза аддитивности частных потерь, обусловленных влиянием каждой отдельной угрозы. Однако механическое следование этой гипотезе может привести к абсурдным результатам. В частности, в нашем примере, принимая гипотезу аддитивности, получаем $q_3 = q_1 + q_2$, что соответствует существенному завышению оценки потерь: «дважды» разрушено одно и то же здание. Более приемле-

мым в этом случае будет применение принципа «большие потери поглощают меньшие», тогда $q_3 = q_2$.

В общем случае на ОР может воздействовать множество из N угроз: thr_1, thr_2,…, thr_N. Если существование этого множества не удовлетворяет требованиям полной группы, совокупность угроз следует трансформировать в множество определенных комплексных событий $Z = \{z_1, z_2, ..., z_n\}$, для которых условия полной группы будут выполняться (см. примеры в п. 1.3). При этом как формирование событий $z_1, z_2, ..., z_n$, так и определение последствий реализации каждого из этих искусственно созданных событий требует внимательного анализа содержания исходной задачи. После формирования полной группы искусственных событий $Z = \{z_1, z_2, ..., z_n\}$, вектора соответствующих вероятностей $P = \{p_1, p_2, ..., p_n\}$ и совокупности последствий (ущерба, потерь) $Q = \{q_1, q_2, ..., q_n\}$ «реализации» этих событий, рассчитывается вектор частных рисков $R = \{r_1, r_2, ..., r_n\}$, где

$$r_i = p_i q_i, \; i = \overline{1,n}. \tag{1.5}$$

Сумма частных рисков равна интегральному риску:

$$R_{\text{int}} = R_{\Sigma} = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i q_i. \tag{1.6}$$

Еще одно замечание по приведенной схеме возникновения и вычисления рисков касается содержания термина «угроза». Слово «угроза» согласно толковому словарю украинского языка [56] употребляется в двух значениях:

− возможность или неизбежность возникновения чего-то опасного, неприятного;

− то, что может причинить какое-нибудь зло, неприятность; опасность.

Очевидно, именно из-за этой двойственности в литературе по «рисковой» тематики термин «угроза» употребляется в обоих смыслах.

В частности, в [57] **угроза (1)** – это угроза-действие, – социальное, природное или техногенное явление, которое приводит к про-

гнозируемым, но не контролируемым нежелательным событиям, которые могут привести к смерти людей или причинить вред их здоровью, повлечь материальные и финансовые убытки, негативно влиять на состояние окружающей среды. Поэтому в перечень угроз входят: землетрясения, наводнения, пожары, войны, эпидемии, загрязнение окружающей среды, аварии на АЭС, предприятиях химической промышленности и др.

Зато в [58] **угроза (2)** – это характеристика возможного влияния рискообразующих факторов опасных явлений и процессов на ОР, степень возможной реализации опасности для ОР. Соответственно имеем: угрозы населению, угрозы территории, угрозы жизни и здоровью людей, угрозы зданиям, помещениям, имуществу.

Интересно, что в некоторых сферах деятельности понятие «угроза» применяется в обоих смыслах. Например, в сфере защиты информации в одних и тех же методических, информационно-справочных изданиях рядом с устоявшимися формулировками «угроза доступности информации», «угроза целостности информации» «угроза конфиденциальности информации» (то есть угрозы в смысле **угроза (2)**) приводятся перечни угроз-действий, в частности в ДСТУ ISO/IEC TR 13335-3:2003 [65] – это **Приложение С (справочное) – Перечень возможных типов угроз**, содержащий перечень случайных или преднамеренных событий, представляющих типичные угрозы как в любой сфере (..., ураган, молния, промышленный влияние, бомбовая атака, ...), так в технической сфере или только в сфере информационных технологий (..., неисправность электропитания ..., нестабильность питания, ..., злонамеренная программная закладка, отказ в обслуживании – DOS-атака, DDOS-атака, ...), в стандарте ISO/IEC 27005:2008 [66] – приложение **Annex C** аналогичного содержания.

Двойственность трактовки термина «угроза» приводит к двусмысленности понимания термина «уязвимость»: для **угрозы (1)** – это наличие в составе ОР неустойчивых, ослабленных элементов, конкретно выделенных и описанных, которые при воздействии на них рискообразующих факторов опасных явлений становятся причиной реализации угрозы-действия, причем механизм реализации очевиден либо детально поясняется; для **угрозы (2)** – это характеристика (описание) возможности причинения каких-либо форм

вреда (потерь, ущерба) ОР в результате реализации угроз относительно ОР без детализации способов осуществления угроз. Собственно перечень этих форм представляет набор обобщенных уязвимостей ОР. Чаще всего такая характеристика задается в виде некоторой статистики, содержащей перечисление обобщенных уязвимостей ОР и соответствующих сведений о частости их реализаций, например: в результате дорожно-транспортных происшествий на дорогах страны в период с ... по … **погибло** … человек, **тяжелые травмы** получило … человек, **травмы средней степени тяжести** – … человек. Здесь угроза (2) – дорожно-транспортные происшествия, объект риска – люди-участники дорожного движения, перечень обобщенных уязвимостей – летальный исход, тяжелые травмы, травмы средней степени тяжести.

Введенные выше категории объекта риска, рисковой ситуации, опасности, источников опасности и т.п. позволяют сформировать достаточно общее описание картины образования и развития рисков.

Рассмотрим произвольный ОР, в отношении которого допустим, что в случае отсутствия каких-либо опасностей его состояние характеризуется вектором параметров X, элементы которого в этом случае принимают свои номинальные значения $[x_{10}, x_{20}, ..., x_{m0}] = X_0$. В этих условиях для ОР гарантируется максимально эффективный режим функционирования, что в соответственно фиксируется номинальным значением комплексного целевого показателя Y качества функционирования этого объекта: $Y_0 = [y_{10}, y_{20},..., y_{k0}]$.

В некоторых случаях вектор $Y = [y_1, y_2,..., y_k]$ удается «свернуть» к скалярному показателю качества φ, что можно отразить введением функционала $\phi = \phi(Y) = \phi(y_1, y_2,..., y_k)$. В условиях отсутствия опасностей $\phi = \phi(Y_0) = \phi_0$.

В случае существования опасности и проявлений порожденных ею угроз происходит ухудшение условий функционирования ОР, состояние которого в этом случае определяется вектором параметров $X_t = [x_{1t}, x_{2t},..., x_{mt}]$, текущие значения x_{it} элементов которого отличны от номинальных. Это различие приводит к ухудшению качества функционирования ОР, фиксируясь в текущих значениях

элементов вектора $Y_t = [y_{1t}, y_{2t}, ..., y_{kt}]$ и уровне скалярного показателя качества $\phi_t = \phi(Y_t)$. Конечным и принципиально существенным звеном в ряде негативных изменений, вызванных влиянием исходной опасности, будут потери (убытки), которые испытывает ОР из-за ухудшения качества своего функционирования. Если эти потери (убытки) предполагают денежную форму представления, она с успехом может быть использована в качестве введенного выше скалярного показатель φ.

В частности, если ОР – предприятие, производящее определенную продукцию, то возможным результатом ухудшения качества его функционирования станет снижение потребительских свойств продукции, падение к ней интереса потребителя, уменьшение спроса и объемов реализации этой продукции, как следствие – текущие финансовые потери предприятия. Если возникшие текущие проблемы не будут преодолены, начнется развитие кризисной ситуации: сокращение или прекращение финансирования предприятии и выполняемых на нем инновационных проектов, технологическое отставание и старение производства, дальнейшее падение потребительских качеств продукции, ухудшение имиджевого положения предприятия, кадровые сокращения и т.п. В приведенном примере достаточно объективный интегральный критерий качества функционирования предприятия может быть сформирован на основе анализа показателей его экономико-финансового состояния, что в принципе позволяет определить конечный (интегральный) убыток предприятия в результате ущерба, нанесенного предприятию реализацией каждой угрозы отдельно.

В условиях точного установления свойств опасностей, в частности порожденной ими совокупности угроз (их детерминирования), существует принципиальная возможность определения фактических характеристик вектора состояния *X*, расчета составляющих вектора целевого показателя качества *Y* и соответствующего значения скалярного показателя φ. Если отклонения двух последних показателей от своих номинальных значений достаточно существенны, принимаются определенные меры по нейтрализации угроз или уменьшению их уровня. Для этого определяются степени и характер влияния каждой из угроз на качество функционирования

ОР (предприятия), формируется профиль рисков, исчисляется интегральный (средний) риск и, согласно последствиям этого анализа, реализуются необходимые корректирующие действия, выполнение которых нормализует условия функционирования ОР. То есть для данной ситуации, когда известна вся информация о характере угроз, их связь с состоянием ОР и качеством его функционирования, присущи вполне осознанные и однозначно детерминированные решения по устранению угроз или уменьшению последствий их реализации до уровней, которые гарантированно обеспечивают нужное качество функционирования ОР (предприятия).

Для получения этого конечного результата предварительно надо решить ряд задач:

1. получить исходную информацию о рисковой ситуации на ОР (предприятии), в том числе данные о характере и уровне опасности, возможности возникновения угроз, перечне и свойствах порождаемых ими деструктивных факторов, характеристиках влияния последних на состояние ОР;
2. определить параметры, отображающие состояние ОР (вектор X);
3. сформировать структуру комплексного целевого показателя Y (или скалярного показателя $\phi(Y)$) качества функционирования ОР (предприятия);
4. вычислить убытки предприятия, обусловленные реализациями отдельных угроз;
5. сформировать профиль рисков;
6. вычислить интегральный риск угроз;
7. принять решение о целесообразности и способах нейтрализации угроз для нормализации условий функционирования ОР (предприятия).

Следует отметить, что ситуация, для которой в полном объеме достигается решение всех приведенных выше задач, на практике фактически не встречается. Главная особенность реально функционирующего ОР – наличие неопределенности при решении любой из указанных выше задач. Источники этой неопределенности разные. Например, различные опасные явления и процессы стохастического характера в среде функционирования ОР, которые обусловлены

действием природных, техногенных и социальных факторов. Если эти факторы действуют одновременно и примерно с одинаково незначительной интенсивностью, имеем «фоновой» уровень опасности, для которого состояние ОР несколько отлично от номинального, о котором шла речь ранее, при этом значения показателей качества работы Y_t или φ_t будут, хотя и в незначительной степени, не совпадать с экстремальными Y_0 или φ_{t0}.

Однако обычно наличие опасности приводит к появлению нескольких «ведучих» угроз, которые и порождают существенные риски, обусловливающие значительные отклонения текущих показателей Y_t и φ_t от экстремальных Y_0 или φ_{t0}. Поэтому в рамках выполнения комплекса вышеперечисленных задач 1)-7) основное внимание следует уделить именно поиску и нейтрализации указанных «ведучих» (общеупотребительный термин – «приоритетных») угроз. Эта задача должна решаться созданной комплексной системой управления рисками – системой менеджмента рисков. Поэтому дополнительно к уже введенным категориям объектов риска ОР, источников опасности ИО, угроз и прочих введем еще одну категорию: **субъекты обеспечения безопасности (СОБ)**. Основными СОБ есть люди, организации, государство, межгосударственные органы. Цель и результаты деятельности СОБ – это создание и сопровождение систем защиты ОР соответствующего уровня:

- системы личной (индивидуальной) безопасности;
- системы корпоративной (коллективной) безопасности;
- системы глобальной безопасности.

Главный результат деятельности СОБ – обеспечение приемлемого для ОР уровня рисков, при котором качество функционирования ОР будет удовлетворять требованиям, установленным для определенной производственной, управленческой или социальной сферы деятельности.

1.2. Неопределеность

Классификация неопределенностей

Среди факторов, влияющих на результат функционирования ОР, большая часть факторов не контролируется лицами, принимающими решения (ЛПР), например, объективные законы природы и об-

щественного развития, которые необходимо учитывать в любом случае, а при их знании – использовать для достижения поставленной цели и учитывать их возможное негативное влияние. Неконтролируемыми являются и другие факторы, например, погодные условия, действия конкурентов, которые относятся к условиям функционирования ОР. Все эти факторы принято называть **неуправляемыми.**

К **управляемым** факторам относят такие, на которые ЛПР может влиять по своему усмотрение, то есть оперировать ими в процессе планирования и осуществления деятельности ОР. К ним относятся, например, факторы, характеризующие способы использования ОР, цель его функционирования. На множестве управляемых факторов формируются стратегии управления ОР.

При исследовании рисков ОР факторы отражаются в виде переменных (числовых и нечисловых). Классификация факторов приведена на рис. 1.1 [58]. С точки зрения осведомленности исследователя о характеристиках факторов последние делят на **определенные и неопределенные.**

К **определенным** факторам относят факторы, значение которых известны исследователю с необходимой точностью. Это различные заданные параметры (константы), известные (регулярные) функции определенных аргументов и т.п. К этой группе факторов также относят контролируемые входные воздействия, в том числе и управляемые переменные.

К **неопределенным** факторам относят переменные, значение которых исследователю не известны или он знаком с ними не полностью. Причина неопределенности этих переменных (факторов) может быть разной. Обычно неопределенные переменные подразделяют на две группы: **случайные** и **неопределенные** переменные нестохастической природы.

При исследовании рисков ОР факторы отражаются в виде переменных (числовых и нечисловых). Классификация факторов приведена на рис. 1.1 [58]. С точки зрения осведомленности исследователя о характеристиках факторов последние делят на **определенные и неопределенные.**

К **определенным** факторам относят факторы, значение которых известны исследователю с необходимой точностью. Это различные

заданные параметры (константы), известные (регулярные) функции определенных аргументов и т.п. К этой группе факторов также относят контролируемые входные воздействия, в том числе и управляемые переменные.

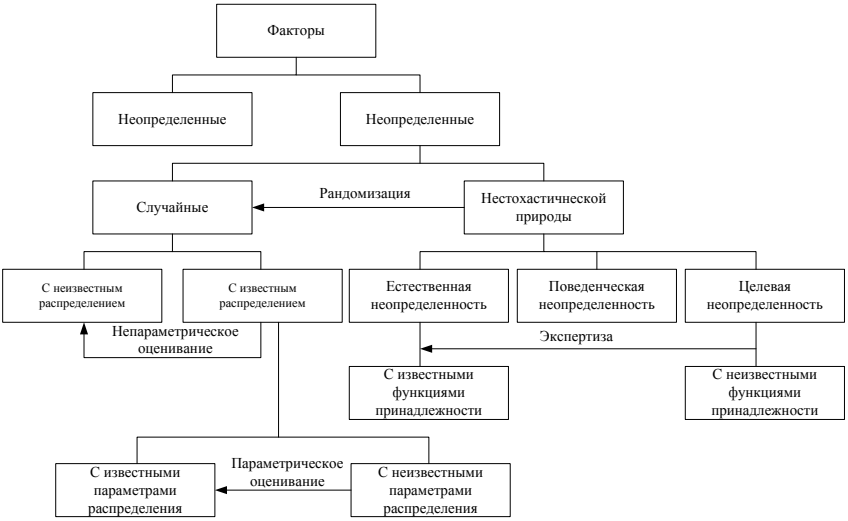


Рис. 1.1. Классификация факторов, влияющих на результат деятельности

К **неопределенным** факторам относят переменные, значение которых исследователю не известны или он знаком с ними не полностью. Причина неопределенности этих переменных (факторов) может быть разной. Обычно неопределенные переменные подразделяют на две группы: **случайные** и **неопределенные** переменные нестохастической природы.

Если распределение случайной переменной (например, в виде функции распределения) известно, то в этом случае говорят, что переменная определена статистически. Случайные переменные с известным распределением подразделяются на два вида: с известными параметрами (характеристиками) распределения и с неизвестными параметрами. При исследовании систем со случайными факторами широко используют статистические методы. Например, методами параметрического статистического оценивания можно определить параметры распределения случайных величин на осно-

ве статистических испытаний (если таковые возможны). Непараметрическое оценивание позволяет описать распределение случайной величины безотносительно к виду закона распределения.

Неопределенные факторы нестохастической природы можно условно разделить на две группы: с известными и неизвестными функциями принадлежности (диапазонами варьирования переменных). Функция принадлежности задает некоторое подмножество общей допустимой области изменения значений фактора, что определяется, например, физическим происхождением соответствующего фактора.

Очевидно, что подмножество (поддиапазон), определяемое функцией принадлежности, в некотором смысле отражает степень неопределенности фактора: чем меньше это подмножество (поддиапазон), тем меньше степень неопределенности. В предельном случае функция принадлежности, выделяющая всего одно значение фактора, переводит его в ряд определенных факторов. Наибольшую степень неопределенности имеют факторы с неизвестными функциями принадлежности. Обычно к ним применяют процедуру экспертной оценки диапазонов изменений их значений.

Для описания **неопределенных** факторов нестохастической природы используют аппарат теории нечетких множеств, субъективные вероятности. В последнем случае при анализе рисков применяют теорию вероятностей. Субъективные вероятности вводят обычно с помощью экспертного оценивания.

Некоторые неопределенности нестохастической природы иногда удается перевести в разряд случайных факторов с помощью **рандомизации**. Под **рандомизацией** понимают искусственное введение случайности в ситуацию, где она отсутствует.

Неопределенность нестохастического характера возникает обычно в результате следующих обстоятельств:

− наличие целенаправленного противодействия со стороны конкурирующей системы, способы действий которой неизвестны исследователю. Эту неопределенность поведения конкурента называют поведенческой неопределенностью;

− недостаточную изученность некоторых явлений, сопровождающих процесс функционирования объекта. Неопределенность этого типа называют «естественной»;

− нечеткое представление цели действия, что приводит к неоднозначной трактовке соответствия полученного реального результата желаемому. Такую неопределенность называют целевой.

Исследование рисков с учетом неопределенных факторов нестохастической природы в значительной степени осложняется отсутствием достаточно общей теории, позволяющей сформировать методологический базис для изучения явлений с неопределенными факторами. Однако использование теории нечетких множеств, теории игр, теории решений позволяет исследовать риски ОР при наличии существенной неопределенности нестохастического характера.

Для практических целей анализа риска введем классификацию неопределенностей результата деятельности по месту расположения относительно ОР, источника происхождения неопределенности, вероятности наступления ожидаемого события и факторов, обусловливающих ее возникновения (рис. 1.2) [58].

Факторы по отношению к исследуемому ОР могут быть **внешними** и **внутренними**. **Внешние** факторы отражают влияние внешней среды на ОР, способствуя успешному проведению определенных действий (полезные факторы) или противодействуя им (вредные факторы). **Внутренние** факторы отражают влияние ситуации, складывающейся внутри ОР, на состояние ОР, процесс его функционирования и результаты его деятельности. Соответственно неопределенности, порождаемые перечисленными факторами, разделяют на **внешние** относительно ОР **и внутренние**, связанные соответственно с внешней и внутренней средой ОР.

Внешняя среда – это макроокружение и непосредственное окружение, в котором функционирует ОР. Например, для организации это среда включает экономическую, правовую, технологическую, социальную, политическую и другие составляющие. В нее включают поставщиков, потребителей продукции и услуг организации, конкурентов, с которыми организация взаимодействует в процессе функционирования.

Внутреннюю среду образует персонал организации, ее структура, производство, финансовое обеспечение деятельности, маркетинг, организационная культура, сложившаяся в организации сис-

тема ценностей, традиции, социально-психологические условия, стиль руководства.

Рис. 1.2. Классификация неопределенностей

По источнику происхождения выделяют следующие составляющие неопределенности информации:

− «**естественную**», обусловленную неполнотой информации, связанной с тем, что в силу объективных причин не все факторы, влияющие на ожидаемый результат, контролируются и прогнозируются, а, следовательно, они должны рассматриваться как случайные;

− «**метрологическую**», обусловленную погрешностями определения (измерения) уровней факторов;

− **поведенческую**;

− **целевую**.

Источником «**естественной**» неопределенности при принятии решений является большое количество обстоятельств, которые невозможно учесть, а их совокупное действие приводит к не вполне предсказуемым результатам. «Естественная» неопределенность связана с невозможностью предсказания в полной мере результата определенной деятельности, так как в подобных условиях, в результате совместного воздействия большого количества случайных

факторов, результаты одного и того же события могут быть разными. Применительно к хозяйственной деятельности можно выделить следующие факторы:

− флуктуации в среде – климатические, погодные условия, стохастический характер природных процессов, времени, места и силы опасных природных явлений, которые могут обусловливать проявления стихийных бедствий и оказать негативное влияние на функционирование и развитие социально-экономической ситуации;

− негативные стохастические процессы в техносфере, связанные с ненадежностью процессов производства (отказами) и эпизодически возникающими опасными техногенными явлениями (пожары, взрывы и т.п.);

− в обществе – нестабильность социально-политической ситуации и неопределенность перспектив ее изменения;

− в экономике – нестабильность деловой окружающей среды, неизмеримо возросшая в процессе экономической глобализации, увеличением числа субъектов деятельности, внедрением современных информационных технологий и большей открытости общества;

− вероятностный характер научно-технического прогресса (НТП): понятны его направления, однако последствия НТП, в частности, результаты научных открытий, известны и прогнозируемы только в сверхшироких пределах;

− нестабильность внутренней среды организации (объем материальных, финансовых и трудовых ресурсов на момент реализации принятого решения и т.п.).

Источники «метрологической» неопределенности – неточности информации об объекте принятия решения, например, недостаточная осведомленность о военном потенциале государства-противника, о величине спроса на товары, услуги и капитал; о финансовой стойкости и платежеспособности клиентов, партнеров, конкурентов; о ценах, курсах, тарифах, дивидендах; о возможности и надежности оборудования; о позициях, способах действий и возможных решения конкурентов и др. Такая информация в практической деятельности является разнородной, неточной, неполной и искаженной. Чем ниже качество информации, используемой при принятии решений, тем более существенные возможные отклоне-

ния фактического результата деятельности от ожидаемых и выше возможность потерь от ошибочных решений.

Поведенческая неопределенность возникает при наличии конфликтных ситуаций, противоборствующих тенденций, столкновений противоречивых интересов: войны, межнациональные конфликты, конкуренция, различие позиций разработчиков, проектировщиков, пользователей и производителей в инновационном процессе. Принятие рациональных решений в этих случаях требует использования специфического математического аппарата теории игр.

Целевая неопределенность возникает в многоцелевых задачах, требующих выбора оптимального решения в условиях многокритериальности. Факторы, обусловливающие возникновение этой неопределенности, подразделяются на:

- природные;
- технические;
- экономические (коммерческие), обусловленные изменениями в экономике предприятия или страны; к ним относятся: неопределенность рыночного спроса и предложения, слабая предсказуемость рыночных цен, неопределенность действий партнеров, недостаток информации о действиях конкурентов и т.д.;
- политические, обусловленные изменением политической обстановки, влияющей на хозяйственную деятельность ОР.

По вероятности наступления анализируемого события и возможности его идентификации рассматриваются три ситуации, которые широко используются в практических задачах принятия решений:

- полной неопределенности (например, времени, места и силы некоторого ативного события), когда определена только область изменения исследуемой величины;
- частичной (вероятностной) неопределенности, например: если известна частота и, следовательно, вероятность негативного события заданной интенсивности в фиксированном месте. Неопределенность такого характера имеет место, когда может быть установлено вероятностное распределение, то есть существует возможность накопить и обработать большое количество статистической информации, что обеспечивает репрезентативность анализируемых выборок;

− полной определенности, которая является чаще предположением, принятым для упрощения расчетов. Следует иметь в виду, что принятие решений на основе анализа, выполненного по детерминированными моделям в предположении, что влияющие факторы известны точно, может привести к потерям из-за ошибок 1-го и 2-го рода, а попытка учета случайного разброса уровней этих факторов значительно усложняет процесс выбора рационального решения.

Показатели неопределенности

Объективный риск как результат взаимодействия человека, общества, техносферы и природы может быть оценен на основе статистики событий, которые произошли, или с использованием теоретико-вероятностных методов и моделей [58]. Для измерения риска необходимы определенные показатели, которые могут быть введены на основе определения риска, и должны отражать три аспекта:

− **неопределенность события:** риск существует только тогда, когда возможно неоднозначное развитие событий. Например, возможность или отсутствие пожара; процентная ставка может вырасти, упасть или остаться на прежнем уровне; стоимость акций может повыситься или снизиться;

− **потери** – непреднамеренное сокращение стоимости объектов в сфере интересов рассматриваемого субъекта в результате реализации опасности. Например, пожар уничтожает дом; в авариях гибнут люди и автомобили; при падении курса акций их владельцы несут убытки. Возможно также непреднамеренное недополучение выгод. Следует отметить, что в наиболее общем случае (спекулятивные риски) рассматривается непреднамеренное изменение стоимости объектов, т.е. учитывается возможный шанс **прироста** этой стоимости;

− **неравнодушие**, то есть риск должен затрагивать интересы конкретного человека или организации, которые стремятся не допустить нежелательного для них развития событий или не «упустить» имеющийся шанс.

В рамках концепции риска как неопределенности, которая широко применяется в различных сферах деятельности, еще не полу-

ченный результат интерпретируется как случайная величина. Поэтому для этой ситуации в качестве характеристик неопределенности (показателей неопределенности), применяются различные характеристики случайной величины.

Допустим, *v* – возможный результат (например, экономический результат – прибыль, доходность и т.д.) определенных действий, операций. Будем рассматривать полученный результат как реализацию значения некоторой непрерывной случайной величины *V*. Ее полной вероятностной характеристикой является функция распределения *F (v) = P (V < v)*. В этом случае ожидаемый результат будет описываться следующими показателями (числовыми характеристиками):

1) *математическое ожидание* $\mu = M[V] = \int_{-\infty}^{\infty} vf(v)dv\mu$, где *f(v)* – плотность распределения вероятностей случайной величины *V*.

Для дискретной случайной величины математическое ожидание определяется по формуле $\mu = \sum_{i=1}^{n} v_i p_i$, где p_i – вероятность *i*-го состояния с ожидаемым результатом v_i. При наличии выборочных данных объемом *n*, если все они считаются равновероятными, т.е. $p_i = 1/n, \ \forall i$, оценкой математического ожидания будет выборочное среднее, которое определяется по формуле $\mu = \frac{1}{n}\sum_{i=1}^{n} v_i$, где v_i – результат, полученный в *i*-м наблюдении;

2) *дисперсия* $D[V] = \sigma^2 = M\left[(V-\mu)^2\right]$, для непрерывной случайной величины рассчитывается по формуле $\sigma^2 = \int_{-\infty}^{\infty} (v-\mu)^2 f(v)dv$, а для дискретной – $\sigma^2 = \sum_{i=1}^{n} (v_i - \mu)^2 p_i$. По выборочным данным несмещенную оценку дисперсии вычисляют по формуле $\sigma^2 = \frac{1}{n-1}\sum_{i=1}^{n} (v_i - \overline{\mu})^2$. Дисперсия учитывает уровень разброса возможных значений случайной величины, являясь характеристикой масштаба ее распределения.

3) среднеквадратическое отклонение $\sigma = \sqrt{D[V]}$;

4) *коэффициент вариации* $K_v = \sigma / \mu$, который имеет смысл риска на единицу среднего результата (относительная безразмерная характеристика).

5) *дифференциальная энтропия* $h = -\int_{-\infty}^{\infty} f(v)\log[f(v)]dv$, для дискретной случайной величины *энтропия* $H = \sum_{i=1}^{n} p_i \log p_i$ где логарифм под знаком интеграла или суммы зачастую может быть двоичным или натуральным. Энтропийный показатель неопределенности чувствителен к форме распределения случайной величины.

Неопределенности и риски

Как отмечалось выше, возникновение, развития, существование риска всегда обусловлено наличием неопределенности или совокупности, комплекса неопределенностей разного рода. Так, в случае установления факта появления опасности – это возможные неопределенности в спецификации совокупности опасных факторов (перечень факторов, вероятность возникновения каждого из них, его возможная интенсивность), неопределенность перечня уязвимостей ОР (в том числе их состав), которые совестно с соответствующими опасными факторами порождают множество угроз для ОР, наконец, неопределенность возможностей реализации этих угроз и последствий (потерь), полученных при их успешной реализации.

В связи с этим важной представляется классификация уровня (степени) неполноты информации в описании рисковой ситуации. Введем качественную шкалу степени неопределенности, которая может возникать в процессе исследования рисковой ситуации:

1. **абсолютная (полная) неопределенность** – отсутствие каких-либо сведений, объясняющих или детализирующих возникшую рисковую ситуацию, например: о совокупности возможных альтернатив (вариантов) развития рисковой ситуации, наличие которых, собственно, и обусловливает возникновение риска; об описании и характеристиках рискообразующих факторов,

которые могут привести к появлению угрозы для ОР; наконец, о составе перечня возможных потерь (убытков), обусловленных успешной реализацией угроз;

2. **неопределенность количественных оценок возможности реализации альтернатив (вариантов)** развития рисковой ситуации, как разновидность этой неопределенности – вводимая часто волевым (субъективным) решением ЛПР **равновозможная неопределенность**, при которой всем возможным альтернативам (вариантам) приписываются одинаковые оценки вероятности реализации;

3. **статистическая (вероятностная) неопределенность адьтернатив** – каждой альтернативе (варианту) развития рисковой ситуации соответствует определенное значение вероятности ее реализации;

4. **неопределенность количественных оценок последствий реализации альтернатив (вариантов)**;

детерминированность – абсолютно полная определенность, т. е. детерминированность ситуации, отсутствие многоальтернативности исходов, точно известные потери.

1.3. Когнитивные модели рисков

Анализ многочисленных материалов, связанных с описанием, исследованием, оцениванием и обработкой рисков, позволяет предположить существование нескольких типизированных групп рисков, в рамках которых интерпретируются практически все известные проявления рисков. Выделяемые группы отличаются друг от друга степенью полноты и уровнем детализации сведений, используемых для описания рисков, актуальных для изучаемого ОР. Для каждой из таких типизированных групп можно сформировать свою концептуальную модель (спецификацию) риска, структура и содержание которой отражают определенный уровень знаний специалиста о предметной области, обеспечивая успешное решение некоторого комплекса прикладных задач из этой предметной области. Подобные модели рисков, адаптированные к уровню восприятия специалистом знаний о предметной области и объему сведений об исследуемом объекте, представляют собой **когнитивные модели**, от лат. *cognitio* – знание, познание.

Фактически когнитивные модели следует рассматривать как набор исследовательских шаблонов со специфическими свойствами и ограничениями, позволяющих применять типовые решения и технологии в соответствующей предметной области.

Модель «опасность – риск»

Данная модель является обобщением значительной группы реальных рисков и рисковых ситуаций. Она базируется на традиционной концепции образования рисковой ситуации как следствия влияния на ОР опасностей различного происхождения, что и обусловливает название модели. В рамках этой модели предполагается известной вся совокупность сведений об угрозах ОР, в частности каждая из них характеризуется вероятностью своей реализации и ущербом, который будет нанесен ОР в случае реализацию соответствующей угрозы.

Возникновение и развитие рисков для модели «опасность-риск» полностью совпадает со схемой (механизмом) образования и развития рисков, приведенной в пп. 1.1. Поэтому остановимся лишь на главных особенностях этой модели.

Во-первых, будем считать, что при анализе возможной рисковой ситуации на ОР в нашем распоряжении есть достоверные сведения об источниках опасностей, рискообразующих факторов и уязвимостей, то есть все данные, необходимые для выявления возможных угроз в понимании **угрозы (2)** и описания рисковой ситуации. Эти данные могут быть представлены кортежем $RS1 = <THR, PR>$, где THR – вектор-перечень возможных угроз, PR – вектор вероятностей реализации каждой из перечисленных угроз. Во-вторых, будем считать известными все данные о последствиях (вектор-перечень CON), возникающие при реализации каждой из угроз, в частности, потери / убытки (вектор Q), обусловленные этими реализациями, которые в совокупности образуют кортеж $<CON, Q>$. Если угрозы thr_1, $thr_2, ..., thr_k$, являющиеся элементами вектора THR, образуют полную группу событий, а вероятности $p_1, p_2, \ , p_k$ реализаций каждой из этих угроз (элементы вектора PR) совпадают с вероятностями возникновения соответствующих потерь / убытков q_1, q_2,

..., q_k , то, вычислив по формуле (1.5) множество частных рисков $r_i = p_i q_i$, $i = \overline{1,k}$ (составляющие вектора рисков R), рассчитаем интегральный риск, который в данном случае, то есть для полной группы событий, равен суммарному риску:

$$R_{\text{int}} = \sum_{i=1}^{n} r_i \ ,$$

являющемуся обобщающей характеристикой состояния безопасности ОР.

В целом спецификация модели «опасность – риск» задается кортежем $< RSQ1 > = < THR, PR, CON, Q, R, R_{\text{int}} >$. С позиций введенной в пп. 1.2 качественной шкалы степени неопределенности отдельные стадии развития риска модели «опасность – риск» могут характеризоваться следующим образом:

− степень неопределенности относительно источников опасностей, рискообразующих факторов, уязвимостей ОР и угроз – **детерминированность;**

− степень неопределенности относительно реализации угроз – **статистическая неопределенность;**

− степень неопределенности относительно последствий реализации угроз и потерь, обусловленных этими реализациями – **детерминированность.**

Таким образом, основные характеристики и свойства модели «опасность – риск» заключаются в существовании акцентированной рисковой ситуации, которую образует множество потенциально опасных негативных явлений и процессов, чье влияние на ОР определяется вероятностями их реализации в виде угроз и обусловленных ими последствий, причиняющих вред ОР. Кроме того, для модели «опасность – риск» характерно наличие полного объема сведений, необходимых для исчисления профиля рисков и суммарного риска угроз, который является интегральной характеристикой уровня опасностей, угрожающих ОР.

В случае неприемлемого уровня интегрального риска (отдельных частных рисков) имеющийся объем сведений достаточен для обеспечения разработки и реализации комплекса мер по нейтрализации угроз и нормализации условий функционирования ОР.

Модель «неопределенность – риск»

Как следует из названия модели, основным источником рисков для данной модели является неопределенность, которая может реализовываться различными способами. В частности, в отличие от предыдущей модели, где рисковая ситуация обуславливалась четко определенным множеством возможных угроз, в модели «неопределенность-риск» о структуре этого множества угроз, видах, формах, механизмах их развития и действия на ОР практически ничего не известно, разве что можно считать вероятным предположение о наличии достаточно значимого влияния совокупности существующих, но не идентифицированных угроз.

Еще один возможный источник неопределенности – недостаточная информация о самом ОР, его структуре, целях и закономерностях функционирования, характеристиках и параметрах. Поэтому часто нет возможности однозначно связать состояние ОР с эффективностью его работы (качеством продукции или услуг на выходе ОР). Обе эти неопределенности практически исключают возможность применения процедуры нормализации состояния ОР путем нейтрализации угроз, влияющих на качество его функционирования.

Рисковая ситуация для модели «неопределенность-риск» формируется на основе сведений о возможности воздействия негативных факторов опасных явлений и процессов на ОР в понимании **угрозы (2)**. Особенностью этой ситуации является то, что она не содержит информации о конкретных способах и формах реализации опасностей, а только данные о последствиях их осуществления. Эти данные представлены в форме описания **угрозы (2)** как возможности или неизбежности нанесения определенного вреда ОР (например, жизни и здоровью людей, зданиям, помещениям, имуществу) вследствие существующей опасности. При этом рассматривается множество характеристик возможных последствий реализации воздействий опасностей с указанием вероятностных характеристик этих последствий, то есть формируется типичная рисковая ситуация. Характерной особенностью представленной таким способом рисковой ситуации является то, что она не позволяет проанализировать непосредственные причины и механизмы возникно-

вения угроз, тем самым фактически исключая возможность предотвращения их возникновения и развития, а также существенно уменьшая зффективность нейтрализации и уменьшению последствий реализации этих угроз.

Рассмотрим схему формирования модели «неопределенность-риск» на примере анализа опасностей дорожного движения.

Во-первых, отметим, что только само участие в дорожном движении уже представляет опасность, которая, в зависимости от обстоятельств, конкретизируется через некоторое множество угроз, то есть участие в дорожном движении – это типичный пример **опасности деятельности**, который является подтверждением рассмотренного выше базового принципа теории рисков – аксиомы потенциальной опасности [58]: любая деятельность таит в себе потенциальную опасность, поэтому объекты, принимающие участие в этой деятельности – это объекты риска, которые при определенных условиях могут понести потери или убытки.

Общий уровень опасности в этом случае можно характеризовать вероятностью совершения дорожно-транспортных происшествий (ДТП). Для определения рисков, как и в предыдущих примерах, следует перейти к анализу вероятностных характеристик конкретных угроз и их возможных последствий. Один из самых простых возможных вариантов исследования угроз безопасности дорожного движения – построение классификация ДТП вида:

1. ДТП, приведших к гибели людей.
2. ДТП, в котором люди получили тяжелые травмы.
3. ДТП, в которых получены травмы среднего уровня тяжести.

……

i. ДТП с повреждением транспортного средства.

……

ДТП, в результате которого произошло повреждение грузаце.

Приведенная выше классификация – это классификация угроз жизни и здоровью людей, угроз целостности транспортного средства и груза в смысле **угрозы (2)**, то есть по степени возможного влияния опасности на состояние ОР в результате реализации этой опасности. Наличие определенной отчетной статистики о ДТП позволяет оценить вероятностные характеристики этих угроз, в итоге получаем ситуацию риска. Однако в отличие от модели «опасность

– риск» в этом случае анализ рисковой ситуации не позволяет проанализировать непосредственные причины возникновения ДТП, ограничивая возможности изучения и исследования угроз безопасности движения формулировкой общих установок и рекомендаций по дорожной безопасности.

В случае, если сведения о характеристиках ДТП имеют более содержательный характер, например, имеется статистика о ДТП в определенном географическом пункте (участке дороги, шоссе), то ее анализ совместно с данными о состоянии дороги в момент ДТП (включая время суток, состояние дорожного покрытия, погодно-климатические условия и т.д.), позволяет получить достаточно детальное описание ДТП и их последствий, допускающее применение статистических методов исследования. Например, это может быть вероятностное распределение $p(k)$, k=0,1,2,… для ДТП, в котором люди получили тяжелые травмы в автомобилях определенного класса в фиксированном промежутке времени при фиксированных условиях состояния дороги, или более обобщенная характеристика, оцененная по той же статистике, но при отсутствии некоторых детализирующих обстоятельств: о времени суток, погодных условиях и пр. В этих случаях рисковая ситуация начинает приобретать черты, характерные для модели «опасность-риск», что позволяет делать более радикальные выводы относительно причин возникновения ДТП и их предотвращению в дальнейшем.

Рисковая ситуация для модели «неопределенность-риск» в подавляющем большинстве случаев формируется именно за счет неопределенности механизмов возникновения и способов реализации угроз, и обычно представляется только множеством возможных вариантов событий-следствий $\{e_i\}$, $i=\overline{1,n}$ воздействия неизвестных деструктивных факторов на ОР и соответствующим множеством $\{p_i\}$, $i=\overline{1,n}$ вероятностей возникновения этих следствий. Типичный пример такой модели можно получить, если обратиться к производственной сфере: пусть $\{e_i\}$, $i=\overline{1,n}$ – варианты бракованной продукции, $\{p_i\}$, $i=\overline{1,n}$ – распределение вероятностей вариантов бракованных единиц продукции. Конкретизируя эту характеристику, можно оценивать распределение для различных рабочих смен, ра-

бочих мест или для различного часа и места работы в пределах каждой смены, что в принципе может помочь выявлению причин брака.

Следует отметить, что для формировании типовой ситуации риска непосредственное описание возможных вариантов последствий реализации угроз в отношении ОР должно быть пересчитано в возможные убытки (потери) предприятия, которые войдут базовыми составляющими в профиль рисков предприятия. К сожалению процедура трансформации последствий воздействия опасных явлений и процессов на ОР в категорию финансового ущерба (потерь) часто оказывается неизвестной или попросту невозможной. Это существенно сужает возможности практического применения модели «неопределенность-риск». Решение этой проблемы зависит от конкретики прикладной области, в которой исследуется риск.

За примером обратимся к сфере технических измерений. Предположим, контролируются значения физической величины – напряжения U, которое в процессе измерения имеет определенное неизменное во времени значение u, неизвестное исследователю. Для измерения применяется цифровой вольтметр, показания которого содержат случайную погрешность. Результат измерений – выборка данных из W последовательно полученных отсчетов измерений прибора: $\{u_t\}$, $t=1, 2, ..., W$. Анализ этой выборки приводит к ранжированному ряду вариантов $u(1) < u(2) < ... < u(n)$ с соответствующими относительными частотами вариантов w_{ri}, $i=\overline{1,n}$, где $w_{ri} = w_i / W$, w_i – частость варианта $u_{(i)}$ в выборке $\{u_i\}$,

$$W = \sum_{i=1}^{n} w_i .$$

Считая относительные частоты w_{ri} оценками вероятностей p_i вариантов, получаем вероятностное распределение $\{u_{(i)}, p_i\}$, $i=\overline{1,n}$. Видим, что имеем типичную рисковую ситуацию: в качестве неизвестного значения u можем взять любой из вариантов, функцию этих вариантов. Как оценить риски того или иного выбора? Как минимизировать эти риски? Эти вопросы решаются методами информационно-статистической теории измерений [67] и более общей теории статистических решений [68].

Естественно предположить, что неизвестное значение напряжения u лежит где-то в пределах замкнутого промежутка $[u_1, u_n]$. В частности, если в качестве неизвестного значения u примем u_1, мы с вероятностью p_1 рискуем допустить ошибку

$$\varepsilon_1 = u_1 - u.$$

Соответственно при выборе варианта u_2 с вероятностью p_2 возможна ошибка

$$\varepsilon_2 = u_2 - u,$$

а в общем случае, для варианта u_i и иметь с вероятностью p_i ошибку

$$\varepsilon_i = u_i - u, \; i = \overline{1,n}. \qquad (1.7)$$

Неверный выбор варианта результата измерений, в зависимости от его дальнейшего использования, может привести к определенному вреду (потерям, убыткам), причем чем больше ошибка ε, тем, скорее всего, более существенным будет этот вред (потери, убытки). Процедура объективного пересчета ошибки ε в категорию финансового убытка обычно неизвестна. Поэтому объем убытков (потерь, ущерба) рассчитывается с применением так называемой функцией потерь $L(\varepsilon_i)$, $i = \overline{1,n}$ [67], которая для данной задачи фактически представляет собой функцию ошибок выбранного в качестве неизвестного значения u варианта результата измерений. Объективный выбор функции потерь является нетривиальной задачей, решение которой требует конкретных знаний о цели и способе применения результатов измерений. Обычно применяют определенные стандартные формы функции потерь, чаще всего $L(\varepsilon_i)$ – квадратичная функция аргумента:

$$L(\varepsilon_i) = (\varepsilon_i)^2 = (u_i - u)^2 = L(u_i - u).$$

Используя именно этот вид функции потерь, проанализируем риски в нашей задаче. Выбор произвольного варианта результата измерений u_i сопровождается возникновением возможных потерь, величина которых определяется соответствующим риском

$$r_i = p_i (u_i - u)^2.$$

Интегрированную оценку возможных потерь по всем вариантам выбора дает средний риск

$$R(u) = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i (u_i - u)^2 , \qquad (1.7)$$

т.е. средний риск – это средние потери в ситуации риска (по всем возможным исходам-вариантам выбора и соответствующими им потерями). Количественные значения p_i, u_i, $i = \overline{1,n}$ в выражении (1.7) известны, поэтому фактический риск $R(u)$ является функцией одного аргумента – u, количественная оценка значения которого есть целью оптимальной обработки полученной выборки $\{u_i\}$. Очевидно, что лучшей будет та оценка u, которая минимизирует средние потери $R(u)$. Применив стандартную процедуру поиска экстремума, получим:

$$\frac{d}{du} R(u) = \frac{d}{du} \{ \sum_{i=1}^{n} p_i (u_i - u)^2 \} = 2 \sum_{i=1}^{n} p_i (u_i - u) .$$

Откуда, приравняв производную 0, найдем решение:

$$u_{opt} = \sum_{i=1}^{n} p_i u_i = \frac{1}{W} \sum_{t=1}^{W} u_t = \bar{u} ,$$

т.е. оптимальной оценкой будет обычное среднее $\bar{u}$.

Следует отметить, что найденная оценка $\bar{u}$ оптимальная только при использовании функции потерь вида (1.6). Другая функция потерь может привести к другой оптимальной оценки u, то есть результат оптимизации имеет субъективный характер. В частности, рассмотрим довольно распространенную модульную функцию потерь вида

$$L(u_i, u) = | u_i - u | . \qquad (1.8)$$

Так как для этой функции не существует производной в точке экстремума, приведенная выше стандартная процедура поиска экстремума не применима для минимизации среднего риска вида

$$R = \sum_{i=1}^{n} p_i | u_i - u | . \qquad (1.9)$$

Чтобы найти оптимальную оценку u_{opt} в этом случае перепишем выражение (1.9) в несколько иной форме:

$$R = \frac{1}{W}\sum_{t=1}^{W} |u_{(t)} - u|, \qquad (1.10)$$

где отсчеты измерений $u_{(t)}$, $t = \overline{1,W}$ – проранжированы в порядке увеличения своих значений выборка. Предположим, что искомая оценка уже известна и для нее выполняется условие: $u_{(k)} \le u_{opt} \le u_{(k+1)}$. Тогда для риска R (формула (1.10)) справедливо представление:

$$R = \frac{1}{W}\sum_{t=1}^{k} (u_{(opt)} - u_{(t)}) + \frac{1}{W}\sum_{t=k+1}^{W} (u_{(t)} - u_{(opt)}). \qquad (1.11)$$

В правой части (1.11) единственной переменной является u_{opt}, реализуем для функции $R(u_{opt})$ типичную процедуру поиска экстремума, в результате которой получаем условие экстремума в виде выражения:

$$\frac{dR}{du_{opt}} = \sum_{t=1}^{k} 1 - \sum_{t=k+1}^{W} 1 = 0. \qquad (1.12)$$

Если n – четное число, то точное выполнение равенства (1.12) происходит в случае, когда каждая из сумм в соотношении (1.12) будет состоять из $k = W/2$ слагаемых, что возможно для:

$$u_{opt} = (u_{(W/2)} + u_{(W/2+1)})/2,$$

т.е. u_{opt} является медианой ранжированы ряда $u_{(t)}$, $t = \overline{1,W}$. В случае, если W – нечетное число, оценка u_{opt} равно медиане $u_{(k)} = u_{((W+1)/2)}$ этого ряда, и, соответственно, получаем $k = (W+1)/2$, а условие (1.12) принимает вид:

$$R = \frac{1}{W}\sum_{t=1}^{k-1} (u_{(opt)} - u_{(t)}) + \frac{1}{W}\sum_{t=k+1}^{W} (u_{(t)} - u_{(opt)}).$$

Если для контроля значения величины U применяется аналоговый измерительный прибор, представленная выше ситуация несколько модифицируется: вместо распределения вероятностей $p(u_i) = p_i$, $i = \overline{1,n}$, используется распределение плотности вероят-

ности *f(u)* непрерывной случайной величины, определенный на интервале значений ($u_{\min}$, $u_{\max}$).

Рассмотрим задачу измерения напряжения в несколько более обобщенной постановке. Будем считать, что неизвестное значение напряжения *x* может лежать в любой точке сегмента [$x_{\min}$, $x_{\max}$], а полученный с помощью аналогового вольтметра результат содержит случайную погрешность *E*:

$$u = x + e.$$

Тогда средние потери при принятии значения u_{opt} за неизвестное истинное значение напряжения определяются условным математическим ожиданием

$$M\{L(x,u_{opt})/u\} = \int_{x_{\min}}^{x_{\max}} L(x,u_{opt}) f(x/u)dx, \qquad (1.13)$$

где $f(x/u)$ – условная плотность вероятности случайной величины *X* при определенном значении *u*, а потери, усредненные по всем возможным показаниям *u*, соответствуют математическому ожиданию

$$M\{L(x,u_{opt})\} = \int_{x_{\min}}^{x_{\max}} \{ \int_{x_{\min}}^{x_{\max}} L(x,u_{opt}) f(x/u)dx\} f(u)du .$$

Очевидно, что лучшей является и оценка u_{opt}, для которой средний риск $M\{L(x,u_{opt})\}$ наименьший. Несмотря на то, что u_{opt} не является переменной внешнего интеграла, можно определить u_{opt} путем минимизации условного среднего риска (1.13). Для квадратичной функции потерь минимизация (1.13) происходит при

$$u_{opt} = \int_{x_{\min}}^{x_{\max}} xf(x/u)dx, \qquad (1.14)$$

а для модульной функции (1.8) – из условия

$$\int_{x_{\min}}^{u_{opt}} f(x/u)dx = \int_{u_{opt}}^{x_{\max}} xf(x/u)dx, \qquad (1.15)$$

то есть, как и в дискретном случае, оптимальными оценками будут среднее (1.14) и медиана, которой соответствует значение верхнего

предела u_{opt} в уравнении (1.15), вычисленные по апостериорному распределению $f(x/u)$ [68]. Отметим, что именно апостериорная условная плотность $f(x/u)$ является характеристикой естественной неопределенности полученного результата измерений u относительно фактического значения напряжения x. Эту характеристику можно выразить через условную плотность $f_e(e/u)$ погрешности измерения e:

$$f(x/u) = f_e(u - x/u).$$

Во многих случаях считается, что распределение $f_e(e/u)$ совпадает с условным распределением $f_e(e/x)$ вероятностей погрешности измерительного средства (в нашем случае – вольтметра). Это распределение может быть найдено экспериментально путем специального исследования (градуировки) измерительного средства. Условием сходимости будет предположение

$$e << x \approx u,$$

которое во многих случаях является вполне оправданным [67].

Отметим, что естественная неопределенность часто является следствием совокупного действия определенного множества случайных факторов, влияние которых в своей массе обусловливает достаточную статистическую устойчивость характеристик этой неопределенности. Поэтому, если указанные характеристики поддаются формализации и допускают возможность своего вычисления или измерения, существует вероятность эффективного решения исходной рисковой ситуации аналитическим путем, через минимизацию специфической формы интегральной оценки риска – так называемого среднего риска, который совместно учитывает и оценивает риски влияния и воздействия всех рискообразующих факторов.

Таким образом, характерной особенностью концептуальной модели «неопределенность – риск» является реальная возможность определения оптимального выхода из рисковой ситуации. К сожалению, этот оптимизм несколько уменьшается, учитывая существующую критериальную неопределенность, которая есть следствием множественности форм функций потерь, и обусловливает возможность появления нескольких разных по значению оптимальных оценок (в приведенном примере – оценок среднего и медианы).

Кроме теории измерений, как приведенные, так и другие оптимизационные схемы для модели «неопределенность – риск» применяются в задачах классификации и распознавания, теории игр, портфельном инвестировании, пр.

Наконец рассмотрим иллюстративный пример, который позволяет предоставить определенную содержательную интерпретацию применению модели «неопределенность – риск» в сфере безопасности предпринимательства [69, 70].

Пусть ОР – объект предпринимательской деятельности (ОПД), относительно которого возможна реализация определенных деструктивных действий, источником которых может быть как внешняя, так и внутренняя среда функционирования ОР. Необходимо провести анализ уровня защищенности ОПД от возможных угроз, оценить величину существующего обобщенного (интегральногй) риска.

Казалось бы, что для решения этой задачи следует прежде всего разработать достаточно полный профиль рисков, и, составив подробный перечень потенциально опасных угроз-действий, дополнив его уязвимостями ОР, актуальными с точки зрения возможной реализации посредством их той или иной угрозы-действия, детально проанализировать механизмы развития каждой из угроз, найдя и исследовав соответствующие цепочки «источник опасности – рискообразующий фактор – уязвимости ОПД – активы ОПД – потери ОПД», затем подсчитать вероятности реализации каждой из угроз, причиненные ею убытки и в конечном итоге оценить частные риски по каждой из угроз. То есть, учитывая изложенное, анализ рисков происходит в рамках применения типовой модели «опасность – риск» путем исследования сценариев развития отдельных частных рисков и перспектив их дальнейшей интеграции в общем рисковом показателе – интегральном риске.

Однако особенность проведения именно такого анализа заключается в том, что он становится очень громоздким и сложным даже при относительно небольшом количестве актуальных угроз-действий и активов, состояние которых критично к реализации хотя бы одной из угроз (более подробно данная проблема рассмотрена в этой монографии в п. 2.2. Практические аспекты определения ценности информации*)*. Кроме того, на практике часто в силу

определенных обстоятельств оказывается невозможным получить данные об источниках опасностей, рискообразующих факторах, а также провести анализ уязвимостей ОР. В этой ситуации доступными для анализа часто остаются только активы организации, что позволяет сформировать перечень угроз, актуальных для организации, однако в отличие от модели «опасность-риск», угрозы в этом перечне – это **угрозы (2)**, то есть угрозы-следствия, которые по своей сути часто являются групповыми угрозами. В основе генерации таких угроз – фрагментация активов ОПД на несколько множеств, каждое включает активы, критические к определенной группе угроз, обобщение которых и приводит к образованию перечня групповых угроз. В частности, для ОПД это может быть:

1. угроза уничтожения имущества и техники, в том числе угрозы физической целостности и исправности технических средств;
2. угроза здоровью и физическому состоянию персонала;
3. угроза в сфере информационной безопасности, связанная с вероятностью несанкционированного доступа в помещение посторонних лиц, нарушениями целостности и конфиденциальности информационных ресурсов;
4. угроза получения убытков в имиджевой сфере и потери репутации (эта угроза трансформируется в сокращение количества заказов, трудности кредитования, пересмотр договорных условий и т.п.).

Таким образом, получаем совокупность из четырех вариантов угроз: V_1, V_2, V_3, V_4, вероятности которых определяются частичными вероятностями p_1, p_2, p_3, p_4, а реализация – соответствующими потерями (табл. 1.2).

Таблица 1.2. Совокупные выходные данные по каждой из угроз ОПД

Варианты угроз	Вероятность реализации угрозы	Ущерб от реализации угрозы
V_1	p_1	q_1
V_2	p_2	q_2
V_3	p_3	q_3
V_4	p_4	q_4

Угрозы V_1, V_2, V_3, V_4 не являются несовместными событиями, они могут происходить одновременно, а могут и не происходить совсем, то есть множество $\{V_j\}, j=\overline{1,4}$ не удовлетворяет требованиям к полной группы событий.

Поэтому возникает задача формирования полной группы $\{Z_i\}$ случайных событий, которые связанны с исходным множеством $\{V_j\}$, но в отличие от него удовлетворяют всем требованиям, предъявляемым к полной группе. Каждое из событий $\{Z_i\}$ $i=\overline{1,m}$ представляет собой совмещение четырех событий (комплексное событие), составленное из элементов множества V_1, V_2, V_3, V_4 и множества дополняющих событий $\overline{V_1},\overline{V_2},\overline{V_3},\overline{V_4}$. Принципиальным при формировании элементарных событий $\{Z_i\}$ $i=\overline{1,m}$ является требование учета в их структуре всех возможных сочетаний элементов этих множеств, включая и комплексное событие, соответствующее ситуация, в которой не реализуется ни одна из угроз.

В процессе формирования событий множества $\{Z_i\}$ должна сохраниться вся информация о возможных состояниях исходной системы угроз $\{V_j\}$, в частности о всех возможных сочетания этих угроз.

В отличие от угроз $\{V_j\}$, $j=\overline{1,4}$, ни одно из событий $\{Z_i\}$, $i=\overline{1,16}$ не может появиться одновременно с другим, только по одному, однако появление одного из событий множества $\{Z_i\}$ является обязательным.

Исходя из этих принципов, для четырех первых элементарных событий имеем:

$$Z_1 = V_1 \cap \overline{V_2} \cap \overline{V_3} \cap \overline{V_4},$$

$$Z_2 = \overline{V_1} \cap V_2 \cap \overline{V_3} \cap \overline{V_4},$$

$$Z_3 = \overline{V_1} \cap \overline{V_2} \cap V_3 \cap \overline{V_4},$$

$$Z_4 = \overline{V_1} \cap \overline{V_2} \cap \overline{V_3} \cap V_4.$$

Учитывая структуру приведенных элементарных событий легко вычислить частные вероятности их реализации. Так для Z_1 получаем: $P(Z_1) = p_1^* = p_1(1-p_2)(1-p_3)(1-p_4)$, формулы для вероятностей p_2^*, p_3^*, p_4^* формируются таким же образом с использованием вероятностей P_j для событий V_j и $(1-P_r)$ для дополняющих событий $\overline{V_r}$. Шесть следующих элементарных событий $Z_5 \div Z_{10}$ содержат попарные сочетания элементов множества $\{V_j\}$, например:

$Z_5 = V_1 \cap V_2 \cap \overline{V_3} \cap \overline{V_4}$,

$Z_6 = \overline{V_1} \cap V_2 \cap \overline{V_3} \cap V_4$,

$Z_{10} = \overline{V_1} \cap \overline{V_2} \cap V_3 \cap V_4$.

Соответственно для вычисления вероятностей этих элементарных событий получаем систему формул:

$$P(Z_5) = p_5^* = p_1 p_2 (1-p_3)(1-p_4),$$

$$P(Z_{10}) = p_{10}^* = (1-p_1)(1-p_2) p_3 p_4 .$$

События $Z_{11} \div Z_{14}$ включают тройные сочетания событий из множества $\{V_j\}$:

$$Z_{11} = V_1 \cap V_2 \cap V_3 \cap \overline{V_4}, \ldots\ldots\ldots, \; Z_{14} = \overline{V_1} \cap V_2 \cap V_3 \cap V_4$$

и характеризуются соответственно вероятностями вида:

$$p_{11}^* = p_1 p_2 p_3 (1-p_4), \ldots\ldots\ldots\ldots, p_{14}^* - (1-p_1) p_2 p_3 p_4 .$$

Структура события Z_{15} учитывает полное сочетание всех событий из множества $\{V_j\}$: $Z_{15} = V_1 \cap V_2 \cap V_3 \cap V_4$, вероятность которого определяется очевидным выражением:

$$p_{15}^* = p_1 p_2 p_3 p_4 .$$

Последнее элементарное событие множества $\{Z_i\}$ должно учесть возможность отсутствия реализации любой из угроз: $\overline{V_1 \cup V_2 \cup V_3 \cup V_4}$, поэтому в терминах исчисления событий имеем:

$$Z_{16}^* = \Omega \setminus \bigcup_{j=1}^{4} V_j .$$

Вероятность этого элементарного события равна

$$p_{16}^{*} = \prod_{j=1}^{4} (1 - p_j).$$

В полном объеме множество структур событий и выражения для вычисления соответствующих вероятностей p_i^*, приведены в табл. 1.3.

В общем случае количество элементов множества определяется формулой:

$$m = \sum_{d=0}^{k} c_k^d = 2^k,$$

где c_k^d – число сочетаний из k элементов по d, в частности для $k = 4$ получаем $m = 16$.

При формировании множества событий $\{Z_i\}$ учтены все возможные варианты развития событий, которые могли бы произойти в ходе реализации угроз (сохранены все возможные сочетания угроз из множества $\{V_j\}$, включая и полное отсутствие угроз), то есть в этом смысле нет потерь информации при трансформировании множества угроз $\{V_j\}$ в множество $\{Z_i\}$.

Комплексные события полного множества $\{Z_i\}$ попарно независимы и образуют полную группу событий, что позволяет применить к ним математический аппарат теории статистических рисков, в частности определять средний риск в форме суммарного риска по формулам (1.6), (1.7). Выражения для вычисления частных ущерба (потерь) $\{Q_i^*\}$, $i = \overline{1,16}$, приняв гипотезу аддитивности частного ущерба, достаточно несложно получить, анализируя логическую структуру событий $\{Z_i\}$. Так для $z_1 = V_1 \cap \overline{V_2} \cap \overline{V_3} \cap \overline{V_4}$ имеем:

$$q_1^* = q(V_1 \cap \overline{V_2} \cap \overline{V_3} \cap \overline{V_4}) = q_1.$$

Соответственно, $q_2^* = q_2, \ldots\ldots\ldots q_4^* = q_4$. Аналогичным образом для событий $z_5 \div z_{10}$ получаем: $q_5^* = q_1 + q_2, \ldots\ldots\ldots, q_{10}^* = q_3 + q_4$, для z_{11}: $q_{11}^* = q_1 + q_2 + q_3$, для z_{15}: $q_{15}^* = \sum_{j=1}^{4} q_j$. Очевидно, что для события z_{16} (отсутствие каких-либо угроз из множества $\{V_j\}$) частный

ущерб отсутствует: $q_{16}^{*}=0$. В упорядоченном виде выражения для вычисления ущерба q_i^{*} приведены в последнем столбце табл. 1.3, которая содержит все данные, необходимые для расчета рисков.

Таблица 1.3. Трансформация «естественного» множества событий $\{V_j\}$, $j=\overline{1,4}$ в полную группу «искусственных» (комплексных) событий $\{Z_i\}$, $i=\overline{1,16}$

Z_i	d	Содержание (структура) события z_i	$P(Z_i)=p_i^{*}$	q_i^{*}
Z_1	1	$(V_1\cup\overline{V}_2\cup\overline{V}_3\cup\overline{V}_4)$	$p_1(1-p_2)$ $(1-p_3)(1-p_4)$	q_1
Z_2	1	$(\overline{V}_1\cup V_2\cup\overline{V}_3\cup\overline{V}_4)$	$(1-p_1)$ $p_2(1-p_3)(1-p_4)$	q_2
Z_3	1	$(\overline{V}_1\cup\overline{V}_2\cup V_3\cup\overline{V}_4)$	$(1-p_1)(1-p_2)$ $p_3(1-p_4)$	q_3
Z_4	1	$(\overline{V}_1\cup\overline{V}_2\cup\overline{V}_3\cup V_4)$	$(1-p_1)(1-p_2)$ $(1-p_3)p_4$	q_4
Z_5	2	$(V_1\cup V_2\cup\overline{V}_3\cup\overline{V}_4)$	$p_1p_2(1-p_3)(1-p_4)$	q_1+q_2
Z_6	2	$(V_1\cup\overline{V}_2\cup V_3\cup\overline{V}_4)$	$p_1(1-p_2)$ $p_3(1-p_4)$	q_1+q_3
....	…	……	……	……
Z_{10}	2	$(\overline{V}_1\cup\overline{V}_2\cup V_3\cup V_4)$	$(1-p_1)(1-p_2)p_3p_4$	q_3+q_4
Z_{11}	3	$(V_1\cup V_2\cup V_3\cup\overline{V}_4)$	$p_1p_2p_3(1-p_4)$	$q_1+q_2+q_3$
Z_{12}	3	$(V_1\cup V_2\cup\overline{V}_3\cup V_4)$	$p_1p_2(1-p_3)p_4$	$q_1+q_2+q_4$
Z_{13}	3	$(V_1\cup\overline{V}_2\cup V_3\cup V_4)$	$p_1(1-p_2)p_3p_4$	$q_1+q_3+q_4$
Z_{14}	3	$(\overline{V}_1\cup V_2\cup V_3\cup V_4)$	$(1-p_1)p_2p_3p_4$	$q_{21}+q_3+q_4$
Z_{15}	4	$(V_1\cup V_2\cup V_3\cup V_4)$	$p_1p_2p_3p_4$	$q_1+q_2+q_3+q_4$
Z_{16}	0	$\Omega\setminus(V_1\cup V_2\cup V_3\cup V_4)$	$(1-p_1)(1-p_2)$ $(1-p_3)(1-p_4)$	0

Далее, используя формулы (1.5) и (1.6), можно вычислить частные риски $r_i = p_i q_i$, $i = \overline{1,15}$ и интегральный риск $R_{\text{int}} = \sum_{i=1}^{15} r_i$, который является обобщающей характеристикой состояния безопасности ОПД.

Исходя из приведенных выше материалов, получаем формальное описание модели «неопределенность – риск» кортежем $< RSQ2 > = < THRCON, PRCON, Q, R, R_{\text{int}} >$, в который, по сравнению с кортежем $< RSQ1 >$, введены новые элементы: $THRCON$ – вектор-перечень **угроз (2)**, то есть угроз-следствий, $PRCON$ – вектор вероятностей этих угроз.

Определяющее отличие модели «неопределенность – риск» состоит в существовании исходной неопределенности относительно механизмов возникновения и развития угроз-действий в отношении ОР. Тем не менее, если на эту исходную неопределенность накладывается ситуативная многовариантность возможных последствий (решений) с количественной оценкой вероятности каждого из них, получаем типичную ситуацию риска.

Учитывая введенную шкалу степени неопределенности отдельных стадий развития риска, модель «неопределенность – риск» может характеризоваться следующим образом:

− степень неопределенности относительно источников опасностей, рискообразующих факторов, уязвимостей ОР и **угроз (1)** (т.е. угроз-действий) – **абсолютная неопределенность;**

− степень неопределенности относительно перечня и содержания множества **угроз (2)** (т.е. угроз-следствий) и потерь, связанных с их реализациями – **детерминированность**.

− степень неопределенности относительно реализации множества **угроз (2) – статистическая неопределенность**;

Модель «возможности – риск / шанс»

Еще одной концептуальной моделью порождения рисков является модель «возможности – риск/шанс». Обычно данная модель применяется для описания ситуаций, возникающих при управлении финансовыми и экономическими рисками, в которых учитывается взаимосвязь между риском и прибылью, когда риск проявляется

как следствие реализации попыток получения максимально возможной прибыли с одновременным ограничением ущерба (потерь). Эта модель рисков характерна для так называемых спекулятивных рисков [59-61, 63], для которых существует вероятность получения как отрицательных (убытки), так и положительных (доходы) результатов, причем последнее, то есть возможность получения положительных результатов, обычно определяется термином «шанс» (согласно [56], **шанс** – вероятность, возможность успеха, осуществления чего-либо).

Подробнее ознакомимся с моделью «возможности – риск / шанс» на примере исследования задачи выбора лучшего из инвестиционных проектов среди множества проектов, заданной кортежем $\boldsymbol{V}= <v_1, v_2, \ldots, v_j, \ldots, v_m>$. Считаем, что возможные условия реализации проектов определяются конечным набором ситуаций, представленных кортежем $\boldsymbol{S}= <s_1, s_2, \ldots, s_i, \ldots, s_n>$, вероятность наступления каждой из которых задается элементом вектора $P=[p_1, p_2, \ldots, p_i, \ldots, p_n]$. Прибыли (или потери), связанные с реализацией проекта v_j в условиях s_i, количественно задаются значением q_{ji} (таблица 1.4).

Таблица 1.4. Исходные данные для задачи выбора лучшего из инвестиционных проектов

Варианты проектов v_i	Варианты условий s_j реализации проектов			
	$\mathbf{s_1}$	$\mathbf{s_2}$	…….	$\mathbf{s_n}$
$\mathbf{v_1}$	q_{11}	q_{12}	…….	q_{1n}
$\mathbf{v_2}$	q_{21}	q_{22}	…….	q_{2n}
……	…….	…….	…….	…….
$\mathbf{v_m}$	q_{m1}	q_{m2}	…….	q_{mn}

Очевидно, что в этой задаче сталкиваемся с двумя ситуациями неопределенности. Первая – типичная ситуация риска, где каждому j-му варианту проекта отвечает множество возможных значений потерь (или прибыли):

$$r_{ji} = p_i q_{ji},\ i \in 1, n\,.$$

Риск или вероятно ожидаемый результат (с учетом возможности как потери, так и прибыли) от реализации j-го проекта составит

$$R_j = \sum_{i=1}^{n} r_{ji} = \sum_{i=1}^{n} p_i q_{ji}\ ,\ \ j = \overline{1,m}\ . \qquad (1.16)$$

Вычислив риски по всем проектам, вновь получаем ситуацию неопределенности. Чтобы выйти из нее, выберем проект, для которого $R_j = \max\ ,\ \ j \in 1,m$. Это будет или наиболее прибыльный, или наименее убыточный проект из всех принятых к рассмотрению вариантов.

Применение модели «возможности – риск / шанс» не ограничивается только финансово-экономической сферой. Эта модель работает везде, где по особенностям практической деятельности возникает потребность в анализе множества возможных вариантов действий, событий, принятия решений и т.п., то есть там, где многоальтернативность рисковой ситуации обуславливается не только влиянием опасностей или действием различных природных факторов, но и создается самим человеком, часто с целью поиска и исследования возможных приемлемых решений в определенной ситуации, сфере деятельности и т.п.

В качестве примера, рассмотрим задачу выбора структуры аппроксимативной модели [71], достаточно актуальную в сфере прикладных применений математических моделей. Объектом риска здесь есть математическая модель реального объекта, который строится по экспериментальным данным, полученным в ходе исследования, изучение или эксплуатации этого объекта [71, 72]. Рисковая ситуация возникает в том случае, когда объект моделирования достаточно сложный, механизм его функционирования неизвестный исследователю (случай так называемой «черного ящика»), из-за чего объективное задание структуры математической модели невозможно. Выход из этой ситуации – построение аппроксимативной модели, которая только формально воспроизводит (имитирует) поведение реального объекта на совокупности экспериментально полученных данных о значении его входных и выходных параметров (переменных, координат и т.п.). То есть при построении аппроксимативной модели не стоит вопрос об определенной содержательно-операциональной близости модели фактическому механизму функционирования объекта. Это приводит к появлению

множества вариантов аппроксимативных моделей, которое, в частности может генерироваться самим исследователем.

Каждому из вариантов модели присущи свои положительные и отрицательные качества – возникает проблема выбора лучшего варианта аппроксимативных модели. Это типичная задача принятия решения [72], содержащая в себе дополнительную неопределенность, обусловленную необходимостью выбора критерия принятия решения (близкая ситуация уже рассматривалась выше для концептуальной модели «неопределенность – риск», где для каждого из двух критериев оптимальности получили свое оптимальное решение). В частности, если в соответствии со структурой таблицы 1.3, множество аппроксимативных моделей определяется элементами кортежа $\boldsymbol{V}$= <v_1, v_2,…,v_j,…, v_m >, множество критериев – кортежем $\boldsymbol{S}$= <s_1, s_2,…, s_i,…, s_n>, а количественные значения соответствующих нормированных критериальных статистик для j-й модели – вектором Q_j=[q_{j1},…,q_{ji},…,q_{jn}], то, при наличии вектора уровней доверия P=[p_1, p_2,…,p_i,…, p_n] каждому из критериев s_i, $i \in 1,n$, выбор наилучшей модели v_{opt} выполняется при условии: $v_{opt} = v_k$, где v_k – модель, для которой статистика (1.16) приобретает экстремальное (максимальное или минимальное, в зависимости от характера критериев) значение.

Учитывая изложенное, можно констатировать, что модель «возможности – риск / шанс» применима для описания и исследования ситуаций, где по особенностям практической деятельности возникает потребность в анализе множества возможных вариантов действий, событий, принятии решений и т.п., то есть там, где многоальтернативность рисковой ситуации обусловливается влиянием различных опасных или наоборот, благоприятных факторов, или создается искусственно с целью поиска, формирования и исследования множества возможных приемлемых решений в определенной ситуации, области деятельности и тому подобное.

Формальное описание модели «возможности – риск / шанс» можно представить в виде кортежа $< RSQ3 > = < V, ST, PRST, Q, R, R_{\text{int}} >$, в котором, по сравнению с кортежами $< RSQ1 >$, $< RSQ2 >$ присутствуют новые элементы: V – вектор-перечень вариантов действий, решений, событий и т.п., ST – вектор-

перечень условий (обстоятельств), при которых происходит реализация анализируемых вариантов, $PRST$ – вектор вероятностей возникновения этих условий (обстоятельств), Q – матрица потерь / доходов. Кроме того, следует отметить изменения в структуре «старых» составляющих кортежа:

R – это матрица частных рисков, структура которой (вплоть до двойных индексов элементов) соответствует структуре матрицы Q, элементы q_{ji} которой в соответствии с выражением (1.16) входят множителем формуле частичного риска r_{ji};

R_{int} – вектор интегральных рисков по каждому из анализируемых вариантов.

Одной из технических особенностей модели «возможности – риск / шанс» является то, что для этой модели характерна неопределенность количественных значений вероятностей возникновения условий (обстоятельств), при которых происходит реализация анализируемых вариантов, в связи с чем довольно распространено применение в элементах вектора $PRST$ субъективных вероятностей.

По введенной шкале степени неопределенности отдельные стадии развития риска модели «возможности – риск / шанс» могут характеризоваться следующим образом:

− уровень неопределенности относительно перечня множества вариантов и потерь / прибылей, связан с их реализациями – **детерминированность.**

− уровень неопределенности относительно возникновения условий (обстоятельств), при которых происходит реализация анализируемых вариантов – **субъективная неопределенность.**

1.4. Базовые понятия управления рисками информационной безопасности

В п. 1.1 был проведен анализ понятия риска в различных предметных областях для последующей его интерпретации в сфере ИБ. Для эффективного осуществления оценивания существующих средств, актуальным является определение таких базовых понятий, связанных с управлением риска, как АОР, угроза и уязвимость. В

этой связи произведен анализ и раскрытие понятий связанных с управлением риском, с последующей интерпретацией в области ИБ и их использованием для анализа существующих методик с целью дальнейшего упрощения их выбора. Понятия АОР в научной литературе и нормативно-правовых документах имеют достаточно широкий спектр трактований и практически часто пересекаются, что видно из нижеследующего анализа понятий [73].

Оценка риска

Оценка риска (risk assessment) (ОР) в некоторых источниках, рассматривается как процесс:

− идентификации ИР системы и угроз этим ресурсам, а также возможных потерь (то есть потенциал потери), основанный на оценке частоты возникновения событий и размере ущерба;

− включающий идентификацию и анализ риска [13, 21, 27, 43, 74];

− выявления риска и определения его влияния [33, 45];

− определения степени потенциальной угрозы и риска, связанного с системой ИТ всюду по ее циклу жизни и развития, включающего в себя 9 шагов (характеристика системы, идентификация угрозы, идентификация уязвимости, анализ контроля, определение вероятности, анализ воздействия, определение риска, рекомендации контроля, документирование результатов) [43];

− составления списка рисков, ранжированных по цене и критичности;

− изучения уязвимостей, угроз, вероятности возможных потерь и теоретической эффективности контрмер;

− оценки угроз, воздействия на уязвимости ИР и процессов, а также вероятности их возникновения [10, 27];

− определения количественными или качественными параметрами величины (степени) рисков [6].

Встречаются и другие определения:

− оценка на постоянной основе вероятности и последствия всех выявленных рисков, с использованием методов, основанных на качественных и количественных оценках (risk evaluation) [41];

− натурально-вещественный и стоимостный анализ всех рисковых обстоятельств, характеризующих параметры риска [7];

− оценка последствий нежелательных событий [75].

Анализ риска

Анализ риска (risk analysis) так же как и оценка, в некоторых источниках, раскрывается как процесс:

− идентификации рисков, определение их величины и выделение областей, требующих защиты (часть управления рисками);

− оценки величины рисков [76];

− систематического использования информации для выявления источников оценки степени риска [45];

− определения источников и количественной ОР [13, 45];

− подробного расследования с целью выявления нежелательных событий [75];

− определение относительной стоимости риска (основанной на последствии) и эффективности системы защиты [47, 77];

− определения угроз безопасности информации и их характеристик, слабых сторон комплексной системы защиты информации (известных и допустимых);

− оценки потенциального ущерба от реализации угроз и степени их приемлемости для эксплуатации автоматизированной системы [38].

После проведения анализа вышеизложенных понятий просматривается некоторая неопределенность относительно точного определения того, что представляет собой АОР и чем эти понятия друг от друга отличаются. Из определений видно, что как оценка, так и анализ связанны процессом идентификации риска.

В ИБ, ОР можно определить как процесс установления значимости риска, после проведения его анализа. В свою очередь для определения анализа риска ИБ наиболее удачным будет использование понятия анализа как процесс идентификации риска в сфере ИБ. И так определив, что АОР является последовательными взаимосвязанными процедурами, рассмотрим понятие управления риском в сфере ИБ.

Управление риском

В научной литературе и нормативных документах касающихся рассматриваемых вопросов встречаются определения понятия **менеджмента или управления риском** (risk management), как скоординированные действия или деятельность:

− по руководству и управлению организацией в отношении рисков (обычно менеджмент риска включает его оценку, обработку, принятие и коммуникацию) [13, 14, 43];

− по сокращению возможных потерь, связанных с риском (в том числе: диверсификация риска, маркетинговые исследования, страхование риска) [78].

Так же, как и понятия АОР в отдельных источниках, под его управлением понимают **процесс**:

− идентификации, управления, устранения или уменьшения вероятности событий, способных негативно воздействовать на ресурсы ИС, уменьшения рисков безопасности, потенциально имеющих возможность воздействовать на ИС, при условии приемлемой стоимости средств защиты (этот процесс содержит анализ риска, анализ параметра «стоимость-эффективность», выбор, построение и испытание подсистемы безопасности, а также исследование всех аспектов безопасности. Цель процедуры управления риском состоит в том, чтобы уменьшить риски до уровней, одобренных DAA (Designated Approving Authority – лицо, уполномоченное выбрать уровни рисков) [27, 79]);

− выявления рисков, ОР и предпринятия шагов по его снижению до приемлемого уровня (включает три этапа – ОР, его снижение и анализ) [45];

− определения приемлемого уровня риска, оценки его текущего уровня, а также выполнения операций по снижению до приемлемого значения и поддержанию последнего [33];

− взвешивания политики альтернатив, с учетом ОР и других факторов, выбора соответствующих профилактик и контроля параметров [74];

− осознания рисков руководством предприятия, определение рисков предприятия и возложения ответственности за управление ими в организации [41];

− включающий в себя набор решений для управления рисками (передача риска, например, через страхование, принятие или уменьшение его посредством выбора соответствующих гарантий) [75];

− осознание причин и границ нежелательных событий, определение приемлемого уровня риска, а также снижение его текущего значения до уровня приемлемого [10].

Базовая цель управления рисками заключается в обеспечении экономического баланса между уровнем рисков на предприятии и стоимостью защитных мер [74].

На основе проведенного анализа указанных определений наиболее оптимальным для отражения понятия управление риском в сфере ИБ будет следующее – согласованные виды деятельности по руководству и управлению организацией в отношении рисков. При этом управление рисками включает в себя все операции, которые можно проводить над риском ИБ:

− минимизация (risk reduction) – выбор и внедрение контрмер по закрытию нарушений базовых характеристик безопасности ресурсов (процесс минимизации риска происходит после его оценки);

− нейтрализация – смягчение риска путем выполнения операций, направленных на противостояние угрозам [33, 45];

− в области ИБ нельзя полностью исключить риски из-за того, что некоторые из них находятся в недосягаемости компании, например, стихийные бедствия, поэтому их принимают (risk retention) – это проводиться, например, с рисками, которые имеют малую вероятность или значимость и приведут к низким затратам;

− остаточный риск или тот, который нельзя полностью перекрыть, обычно ответственность за него передают третьему лицу, передача риска или страхование (risk transfer) – это система мер по защите интересов физических и юридических лиц за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов [80, 81].

По анализу операций, которые можно производить над рисками, можно сделать вывод, что все они объединяются таким понятием как управление риском [54, 56].

1.5. Международные стандарты в области анализа и оценивания рисков

Для определения типов входных, внутренних и выходных параметров, которые используются для АОР, осуществим исследование соответствующей современной нормативной базы.

Стандарт NIST 800-30

Стандарт NIST 800-30 [82] (Risk Management Guide for Information Technology Systems, разработчик – NIST, США) охватывает девять первичных шагов:

- характеристика системы;
- идентификация угроз (табл. 1.5) [82];

Таблица 1.5. Пример идентификации угроз

Источник угрозы	Причина	Действие угрозы
Хакер, крекер	Вызов, Эго, Бунт	Хакинг, социоинжиниринг, вторжение и взломы, несанкционированный доступ (НСД) в ИС.
Кибер-преступник	Разрушение информации, Информационное раскрытие, Несанкционированная модификация данных (НМД)	Компьютерное преступление (кибер-преследование), Мошеннические действия, Информационный подкуп, Spoofing, Вторжение в ИС

- идентификация уязвимостей (табл. 1.6) [82];
- анализ управления;
- определение вероятности;
- анализ воздействия;
- определение риска;
- рекомендации по управлению;
- документирование результатов.

В процессе анализа риска производится сбор информации, идентификация угроз (определение источника, причины и действия угрозы). Для оценки используются следующие уровни вероятности:

- высокий «В»,
- средний «С»,
- низкий «Н».

Таблица 1.6. Пример идентификации пары уязвимость-угроза

Уязвимость	Источник угрозы	Действие угрозы
ID уволенных служащих не удалены из ИС	Уволенные служащие	Проникновения в ИС на основе личных данных
Брандмауэр компании разрешает входные соединения telnet и на сервере XYZ включен ID гостя	Несанкционированные пользователи (например, хакеры, уволенные служащие)	Использование telnet для доступа к серверу XYZ и чтение системных файлов по ID гостя

При анализе воздействия определяются события, связанные с потерей К, Ц и Д. Величина воздействия определяется по шкале:

- высокая (В),
- средняя (С),
- низкая (Н).

Для определения риска используется матрица УР: «В»; «С»; «Н» (табл. 1.7) [82].

Таблица 1.7. Матрица УР

Вероятность угрозы	Воздействие		
	Н (10)	***С (50)***	***В (100)***
В (1,0)	**Н** 10 × 1,0 = 10	**С** 50 × 1,0 = 50	**В** 100 × 1,0 = 100
С (0,5)	**Н** 10 × 0,5 = 5	**С** 50 × 0,5 = 25	**С** 100 × 0,5 = 50
Н (0,1)	**Н** 10 × 0,1 = 1	**Н** 50 × 0,1 = 5	**Н** 100 × 0,1 = 10

BSI-Standard 100-3

BSI-Standard 100-3 [44] (Risk Analysis based on IT-Grundschutz – анализ рисков на основе IT-Grundschutz, разработана Federal Office for Information Security – BSI, Германия) основывается на процессе АОР IT-безопасности, предложенного в BSI-Standard 100-3-й, включает семь этапов.

Этап 1 – Предварительная подготовка. На этом этапе определяется область ИБ, требования к ней (нормальные, высокие и очень высокие), которые рассматриваются с точки зрения обеспечения К, Ц и Д.

Этап 2 – Подготовка описания угрозы. С помощью предложенного в методике списка угроз осуществляется их анализ для кон-

кретного предприятия. Идентифицируются модули и целевые объекты (ЦО) защиты, которые заносятся в таблицу (табл. 1.8) [44].

Таблица 1.8. Пример идентификации

№	Название модуля	ЦО
B 2.4	Серверная комната	Каб. М. 723
B 2.6	Производственная комната	Каб. М. 811
B 3.101	Сервер	S3
B 3.207	Главный клиент	C4
B 3.301	Шлюз безопасности (Firewall)	N3

Каждый модуль ЗИ связан со списком угроз, а номер и их название соответствует конкретному ЦО.

Результатом прохождения этапа является список угроз конкретному объекту (табл. 1.9) [44]. Далее в обобщенной таблице угрозы сортируются по каждому ЦО.

Таблица 1.9. Пример описания угроз

Сервер S3
К: нормальная; Ц: высокая; Д: высокая
Т 1.2 Отказ IT-системы, Т 3.2 Неумышленное уничтожение актива, Т 4.1 Перебой в питании, Т 5.57 Сетевое сканирование, Т 5.85 Потеря Ц информации и т.д.

Этап 3 – Определение дополнительных угроз.

Этап 4 – Оценка угрозы (ОУ). Здесь производится тематический опрос специалистов на основе базовых запросов. Результаты фиксируются в таблице с указанием Y (если меры ИБ (осуществленные или предусматриваемые) обеспечивают надлежащую защиту от соответствующей угрозы или, что угроза не важна для текущего анализа степени риска) или N (если меры ИБ (осуществленные или предусматриваемые) не обеспечивают надлежащую защиту от соответствующей угрозы) для каждой отдельной угрозы (табл. 1.10)) [44].

Этап 5 – Обработка рисков. Здесь используется шкала:

- «А» – снижение риска посредством дополнительных мер;
- «В» – предотвращение риска посредством реструктурирования;
- «С» – принятие риска;

− «D» – передача риска (табл. 1.11) [44].

Этап 6 – Консолидация концепции ИБ.

Таблица 1.10. Пример ОУ

Сервер S3	**ОУ**
К: нормальная; Ц: высокая; Д: высокая	
Т 1.2 Отказ IT системы	N
Меры ИБ для сервера S3 не предотвращают реализацию угрозы. IT – меры по Каталогу Grundschutz не соответствуют	
Т 5.85 Потеря Ц информации	N
Информация клиента о заказе не должна подвергаться несанкционированная модификация (НСМ).	

Этап 7 – Обратная связь [44].

Таблица 1.11. Пример таблицы обработки риска

Сервер S3	
К: нормальная; Ц: высокая; Д: высокая	
Т 1.2	Отказ IT-системы
«*A*» S 6. U1	Дополнительная IT-мера по ИБ: Осуществление полной замены системы для общения с клиентом. Реализуется полная замена системы для связи с клиентами. Резервная система располагается в помещении Е.3. с возможностью использования в любой момент времени, (не > 30 мин. задержки производства).

Стандарт РС БР ИББС-2.2-2009

Стандарт РС БР ИББС-2.2-2009 [83] (Рекомендации в области стандартизации Банка России, обеспечение ИБ организаций банковской системы, Российская Федерация) АОР нарушения ИБ проводится для типов информационных активов (ИА), входящих в предварительно заданную область оценки. На начальном этапе определяются:

− полный перечень типов ИА, входящих в область оценки (на основе результатов их классификации);

− полный перечень типов объектов среды, соответствующих каждому из типов ИА области оценки;

− модель угроз ИБ, основанной на всех выделенных типах объектов среды всех уровней иерархии информационной инфраструктуры.

Процесс ОР нарушения ИБ осуществляется на основании качественных (КЧ) оценок вероятности реализации угрозы (в оригинале СВР – степень возможности реализации угроз ИБ) и потенциального ущерба от ее реализации (в оригинале СТП – степень тяжести последствий от потери свойств ИБ для рассматриваемых типов ИА). Оценка определяется на основе экспертного мнения специалистов службы ИБ с привлечением профессионалов в области IT. Для проведения ОР нарушения ИБ выполняются 6 процедур:

1. Определение перечня типов ИА, для которых выполняется оценка (т.е. области ОР). Для каждого типа ИА следует определить, какие для него свойства ИБ (К, Ц, Д и, при необходимости, другое) должны быть обеспечены;

2. Определение перечня типов объектов среды (разделяются по уровням информационной инфраструктуры) соответствующих каждому из типов ИА;

3. Определение перечня актуальных источников угроз (формируется на основе модели угроз компании) для каждого из указанных типов;

4. Определение СВР угроз в отношении типов объектов среды. На основе пятиступенчатой КЧ шкалы («нереализуемая» (НР), «минимальная» (МН), «средняя» (СР), «высокая» (ВС), «критическая» (КР)) проводится анализ возможности потери свойств ИБ для каждого из типов ИА в результате воздействия угроз. Основными факторами для оценки СВР угроз ИБ является: информация от соответствующих моделей угроз (данные о расположении источника угрозы его мотивации и предположения о квалификации (ресурсах) источника), статистические данные о частоте реализации угрозы ее источником в прошлом, информация о способах осуществления угроз и сложности их обнаружения, а также данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер;

5. Определение СТП для типов ИА на основе анализа последствий потери каждого из значимых свойств ИБ для каждого из типов ИА в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз. Используется четырехступенчатая КЧ шкала («МН», «СР», «ВС», «КР»).

Основными факторами для оценивания являются:

− степень влияния на непрерывность и репутацию деятельности компании;

− объем финансовых (материальных) потерь и затрат на восстановления свойств ИБ ИА (ликвидации последствий нарушения ИБ – финансовых, материальных, временных и людских ресурсов);

− степень нарушения законодательных требований (договорных обязательств компании), а также требований регулирующих и контролирующих органов в области ИБ;

− объем хранимой, передаваемой, обрабатываемой и уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;

− данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих защитных мер, снижающих тяжесть последствий (апостериорных);

6. Оценивание рисков нарушения ИБ проводится на основании сопоставления СВР угроз и СТП нарушения ИБ вследствие реализации соответствующих угроз. Оценка проводиться для всех значимых свойств ИБ выделенных типов ИА, всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз. Используется следующая КЧ шкала рисков: допустимый (Д), недопустимый (НД). Для сопоставления СВР угроз и СТП заполняется таблица Д и НД рисков нарушения ИБ (табл. 1.12) [83].

Таблица 1.12. Д и НД риски

СВР угроз ИБ	**СТП нарушения ИБ**			
	МН	**СР**	**ВС**	**КР**
НР	Д	Д	Д	Д
МН	Д	Д	Д	НД
СР	Д	Д	НД	НД
ВС	Д	НД	НД	НД
КР	НД	НД	НД	НД

Риски нарушения ИБ могут быть оценены в количественной (КЛ) (денежной) форме на основании оценок СВР угроз ИБ (например, в %) и СТП (например, в денежном виде от величины капитала компании (ВКК)).

Количественные оценки также производятся экспертными методами.

При необходимости, могут использоваться шкалы (табл. 1.13) [83] соответствия КЧ и КЛ оценок СВР угроз и СТП.

Таблица 1.13. Шкалы соответствия

СВР угрозы		СТП нарушения ИБ	
($М_{кч}$)	($М_{кл}$), %	($М_{кч}$)	($М_{кл}$), %
НР	0	МН	[0; 0,5[
МН	]0; 20[	СР	[0,5; 1,5[
СР	[20; 50[	ВС	[1,5; 3,0[
ВС	[50; 100[	КР	[3,0; 100] (от ВВК)
КР	100		

Количественные ОР нарушения ИБ является произведением оценок СВР угроз и СТП для каждого из значимых свойств ИБ выделенных типов ИА и всех соответствующих им комбинаций объектов среды и воздействующих на них источников угроз. Суммарная ОР компании вычисляется как сумма КЛ оценок по отдельным рискам нарушения ИБ. Также в методике есть перечни рекомендуемых классов и источников угроз ИБ [83].

Стандарт ISO/IEC 27005:2008

Стандарт ISO/IEC 27005:2008 [84, 85] (Information technology – Security techniques – Information security risk management (Информационная технология – Методы защиты – Менеджмент рисков ИБ) представляет технический пересмотр стандартов, отмену и замену ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000, Швейцария) предоставляет рекомендации для менеджмента риском ИБ организации, в особенности поддерживая требования «Системы менеджмента информационной безопасности» (ISMS) согласно ISO/IEC 27001. Процесс менеджмента реализуется в шесть этапов [86, 87].

Этап 1 – Создание контекста. Осуществляется общий анализ всей информации об организации, относящейся к созданию контекста, а также производится установка основных критериев, необходимых для менеджмента рисков ИБ и определение для него области применения и границ осуществления.

Этап 2 – ОР. Здесь осуществляется идентификация (активов, угроз, существующих требований, уязвимостей и последствий), оценка и описание (КЛ, КЧ или их комбинация), расположение по приоритетам рисков, относящимся к организации. Качественная оценка использует шкалу квалификации атрибутов, чтобы описать величину потенциальных последствий (например, низкие, средние или высокие) и вероятность, что эти последствия произойдут. Количественная оценка использует масштаб с числовыми значениями, как для последствий, так и вероятности. Количественная оценка в большинстве случаев использует статистику инцидентов. Результатами прохождения данного этапа будут оценки последствий, вероятности инцидента и УР.

Этап 3 – Обработка рисков. Включает общее описание обработки, а также снижение, сохранение, предотвращение и перенос риска.

Этап 4 – Принятие риска.

Этап 5 – Коммуникации риска.

Этап 6 – Мониторинг и пересмотр риска ИБ.

Здесь осуществляется мониторинг и пересмотр факторов риска, а также улучшение его менеджмента. В стандарте присутствуют рекомендации и примеры:

− определения области применения и границ процесса менеджмента рисков (Приложение А);

− идентификации и определения ценности активов, стоимости воздействия (Приложение В);

− типичных угроз (Приложение С, табл. 1.14 [85], где метки имеют следующее значения: D – преднамеренный (намеренные акции, нацеленные на ИА), А – случайный (непреднамеренные действия человека на ИА) и Е – экологический (инциденты, которые не основаны на действиях человека));

Таблица 1.14. Пример типичных угроз

Тип	Угрозы	Метки
НСД	Несанкционированное использование оборудования	D
	Мошенническое копирование программного средства (ПС)	D
	Использование поддельных или скопированных ПС	A, D
	Искажение данных	D
	Незаконная обработка данных	D

− уязвимостей и методы их оценивания (Приложение D, см. пример уязвимостей для аппаратных средств в табл. 1.15 [85]);
− подходов к ОР (Приложение E, табл. 1.16 – 17 [85]);
− ограничения по снижению риска (Приложение F).

Стандарт имеет реализации в ПС, например, Meycor KP (Knowledge Provider). В ISO/IEC 27005:2008 предложена высокоуровневая и детальная ОР ИБ.

Таблица 1.15. Примеры уязвимостей и угроз

Уязвимости	Угрозы
Недостаточное обслуживание (дефектная инсталляция)	Брешь в возможности ремонта ИС
Изъяны схем для периодических замен	Разрушение оборудования (носителей)
Изъяны эффективного контроля внесения изменений конфигурации	Ошибка в использовании
Восприимчивость к перепадам питания	Потеря источника питания

Для последней может использоваться матрица с предопределёнными значениями (см. табл. 1.16 [85]). Для каждого актива рассматриваются соответствующие уязвимости и угрозы, например, если ценность актива – ЦА = 3, ВВ угрозы – ВВУ = «В» и простота использования уязвимости – ПИУ = «Н» то мера риска – МР = 5.

Таблица 1.16. Матрица оценки МР

ВВУ		**Н**			**С**			**В**		
ПИУ		**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
ЦА	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	**5**	6	7
	4	4	5	6	5	6	7	6	7	8

Также предложена матрица определения вероятности сценария инцидента (ВСИ) (см. табл. 1.17 [85], где «ОН» (очень низкая), «Н» (низкая), «С» (средняя), «В» (высокая), «ОВ» (очень высокая)), что соответственно означает (очень маловероятно), (маловероятно), (возможно), (вероятно), (часто).

Получаемое в результате значение риска измеряется по шкале от 0 до 8 (например, «Н» (0-2); «С» (3-5); «В» (6-8)), может быть оценено относительно критериев принятия риска. В приложении стандарта рассмотрен пример ранжирования угроз посредством мер риска (МР) (см. табл. 1.18 [85]).

Таблица 1.17. Матрица определения ВСИ

	ВСИ	ОН	Н	С	В	ОВ
Влияние на бизнес	ОН	0	1	2	3	4
	Н	1	2	3	4	5
	С	2	3	4	5	**6**
	В	3	4	5	**6**	**7**
	ОВ	4	5	**6**	**7**	**8**

Матрица может использоваться, для связи факторов последствий (ЦА) с ВВУ (принимая в расчет аспекты уязвимости). Изначально по определенной шкале (например, 1 ÷ 5) производится оценка ЦА для каждого находящегося под угрозой актива (колонка (b)).

Далее, например, по той же шкале оценивается ВВУ, для каждой угрозы (колонка (c)) и по полученным результатам вычисляется мера риска (колонка (d)) путем умножения $d = b \times c$. Впоследствии проводится ранжирование угроз (колонка (e)) в порядке соответствующей меры риска (в табл. 1.18 [85] 1 – самое низкое последствие и самая низкая ВВУ. В колонке (a) отображены идентификаторы угрозы).

Таблица 1.18. Пример ранжирования угроз

(a)	**(b)**	**(c)**	**(d)**	**(e)**
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5
E	4	1	4	4
F	2	4	8	3

Рассмотрим пример, в котором особое внимание уделяется последствиям инцидентов ИБ и определению того, каким системам следует отдавать предпочтение. Это выполняется путем оценки

двух значений для каждого актива и угрозы, комбинация которых будет определять баллы ($Б_{ij}$), где i и j – соответственно номер актива и угрозы. Суммирование всех баллов активов дает возможность определить МР. Сначала каждому активу присваивается ЦА для каждого случая возникновения соответствующей угрозы. Далее определяется показатель вероятности риска (ПВР). Он оценивается исходя из комбинации ВВУ и ПИУ (см. табл. 1.19 [85]).

Таблица 1.19. Пример оценки

ВВУ	**Н**			**С**			**В**		
ПИУ	Н	С	В	Н	С	В	Н	С	В
ПВР	0	**1**	2	1	2	**3**	2	3	4

Затем по пересечению линий значений ЦА и ПВР в табл. 1.20 [85] присваиваются соответствующие баллы. После чего они подсчитываются, для получения итоговых значений по каждому активу. Далее предположим, что система С имеет три актива $А_1$, $А_2$, $А_3$ и существуют две угрозы $У_1$, $У_2$ этой системе. Пусть $ЦА_1 = 3$, $ЦА_2 = 2$ и $ЦА_3 = 4$. Если для $А_1$ и $У_1$ $ВВУ_{11}$ = «Н» и $ПИУ_{11}$ = «С», то значение $ПВР_{11} = 1$ (см. табл. 1.19 [85]).

Таблица 1.20. Балльник

ПВР	**ЦА**				
0	0	1	2	3	4
1	1	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	**6**	7
4	4	5	6	7	8

Баллы для $А_1$ и $У_1$ могут быть выведены из табл. 1.20 [85] на пересечении линий $ЦА_1 = 3$ и $ПВР_{11} = 1$, т.е. $Б_{11} = 4$. Аналогичным образом, пусть для $А_1$ и $У_2$ $ВВУ_{12}$ = «С», а $ПИУ_{12}$ = «В», то $ПВР_{12} = 3$ т.е. $Б_{12} = 6$. Теперь могут быть вычислены итоговые баллы ($БИ_i$) актива относительно всех угроз $БИ_1=Б_{11}+Б_{12} = 10$.

Вычисление итоговых баллов по всей системе (БИС) производится путем суммирование всех баллов по каждому активу относительно всех угроз $БИС=БИ_1+БИ_2+БИ_3$ [85]. В стандартах ISO/IEC 27001 и 27002 на этапе ОР ИБ дается ссылка на документ ISO/IEC TR 13335-3, который теперь представлен как ISO/IEC 27005.

Стандарт AS/NZS 4360:2004

Стандарт AS/NZS 4360:2004 [88] (Австралия и Новая Зеландия) предоставляет рекомендации по АОР, которые проводится в 7 этапов.

1. Определение контекста оценки степени риска.

2. Идентификация риска основывается на инициализации табл. 1.21 [88].

Таблица 1.21. Идентификация и анализ риска

Ссылка риска	**Риск** Что может произойти?	**Источник** Как может это происходить?	**Воздействие от реализации риска**	**Текущие стратегии управления и их эффективность** (А) – адекватные; (М) – умеренные; (I) – недостаточные.	**УР** Вероятность	**УР** Последствие	**УР** Текущий УР	**Приемлемость**

3. Анализ степени риска. Определяются последствия (L), вероятность (P) и УР с помощью матрицы риска (табл. 1.22 [88]).

4. ОР. Сравниваются оцененные УР с предустановленными критериями.

5. Обработка риска.

6. Контроль.

7. Консультации [88].

Моделирование процесса риск-менеджмента целесообразно проводить на базе требований стандарта Австралии и Новой Зеландии AS/NZS 4360:2004 «Риск-менеджмент». Разработку данного нормативного документа осуществлял Объединенный технический комитет ОВ-007 «Риск-менеджмент», состоящий из представителей «Стандартов Австралии» и «Комитета по Стандартам Новой Зеландии». В составе комитета представлены двадцать четыре организации, являющимися в Австралии и Новой Зеландии ведущими в сфере управления рисков.

Принципы, заложенные в этом стандарте, органично вписываются в процессно-ориентированную модель системы управления организацией. Целью стандарта AS/NZS 4360:2004 «Риск-менеджмент» является определение общих требований для выявления условий возникновения, идентификации, анализа, оценки, обслуживания, мониторинга рисков и обмена информацией о рисках.

Таблица 1.22. Пример матрицы риска

где, E – Чрезвычайный риск (необходимо детализировать требуемый план действий);
H – Высокий риск (необходимо внимание высшего руководства);
M – Средний риск (определяет управленческую ответственность);
L – Низкий риск (обрабатывается обычными процедурами).

					Последствие				
				Бизнес-процесс& Системы	Незначительные ошибки в системах или процессах, требующих корректирующего действия, или незначительной задержки без воздействия на полный график.	Стратегическая процессуальная норма, время от времени не встречается или услуги, не полностью удовлетворяют потребностям.	Одно или более ключевых требований не будут выполнены.	Стратегии не совместимые с повесткой дня правительства. Тенденции показывают, что обслуживание ухудшается	Критический системный отказ, плохой стратегический план или продолжающееся несоблюдение. Бизнес серьезно пострадал.
				Финансовые	1% от бюджета или <$5 тыс.	2.5% от бюджета или <$50 тыс.	> 5% от бюджета или <$500 тыс.	> 10% от бюджета или <$5 мил.	>25% от бюджета или >$5 мил.
					Незначительное	**Малое**	**Умеренное**	**Большое**	**Катастрофическое**
	Вероятность	**Статистика**			**1**	**2**	**3**	**4**	**5**
Вероятность	> 1 при 10	Произойдет в большинстве случаев	**5**	**Почти бесспорно**	**M**	**H**	**H**	**E**	**E**
	1 при 10 - 100	Вероятно, произойдет	**4**	**Вероятно**	**M**	**M**	**H**	**H**	**E**
	1 при 100 – 1 000	Могут возникнуть в будущем	**3**	**Возможно**	**L**	**M**	**M**	**H**	**E**
	1 при 1 000 – 10 000	Могут произойти, но сомнительно	**2**	**Врядли**	**L**	**M**	**M**	**H**	**H**
	1 при 10 000 – 100 000	Могут произойти при исключительных обстоятельствах	**1**	**Редко**	**L**	**L**	**M**	**M**	**H**

Требования AS/NZS 4360:2004 должны применяться при выполнении любых функций организации, на всех этапах реализации проектов, стадиях жизненного цикла продукции и т.д. AS/NZS 4360:2004 может применяться к различным видам деятельности любой государственной, частной или общественной организации, а также к действиям отдельных людей. Стандарт определяет основные требования к процессу управления рисками и, как следствие, не связан конкретно с определенной отраслью промышленности или экономики. Форма и способ применения управления рисками будут зависеть от меняющихся потребностей организации, ее кон-

кретных целей, продукции и услуг, а также внутренних процессов и специфики деятельности.

Стандарт AS/NZS 4360:2004 является третьей версией стандарта. Две предыдущие были опубликованы в 1995 и 1999 годах. По сравнению с версией 1999 года в новой редакции стандарта сделан больший акцент на внедрение управления рисками в практическую деятельность организаций, а также на управление потенциальной выгодой и возможными убытками. В этом стандарте государственным, частным или общественным организациям, группам или частным лицам предложено руководство для: создания надежной базы для принятия рисковых решений и планирования; идентификации перспектив и опасностей; получения выгоды от неопределенности предпринимательской среды; построения системы управления, ориентированной на предупреждение потенциальных проблем, а не на коррекцию последствий после их возникновения; эффективного распределения и использования ресурсов; улучшения антикризисного управления и сокращения убытков и расходов на риск, включая взносы за коммерческое страхование; укрепления доверия заинтересованных сторон; соответствия нормам действующего законодательства; совершенствования корпоративного управления; моделирования процесса риск-менеджмента.

Структурная схема процесса риск-менеджмента [89] представлена на рис. 1.3.

Более подробно каждая стадия процесса риск-менеджмента рассмотрена в следующих разделах. Основные структурные элементы процесса риск-менеджмента отражены в табл.1.23 [89, 90].

Риск-менеджмент можно применять на разных уровнях организации: стратегическом, тактическом (уровень руководителей второго звена), а также операционном. Он может быть использован в отдельных проектах, при поиске необходимых решений при управлении отдельными зонами риска. На каждой стадии процесса следует вести записи, позволяющие регистрировать информацию о функционировании процесса риск-менеджмента, необходимую для контроля и улучшения этого процесса. В широком смысле управление риском основывается на **концепции приемлемого риска**, на возможности влияния на начальный уровень риска с целью доведения этого уровня до приемлемого значения.

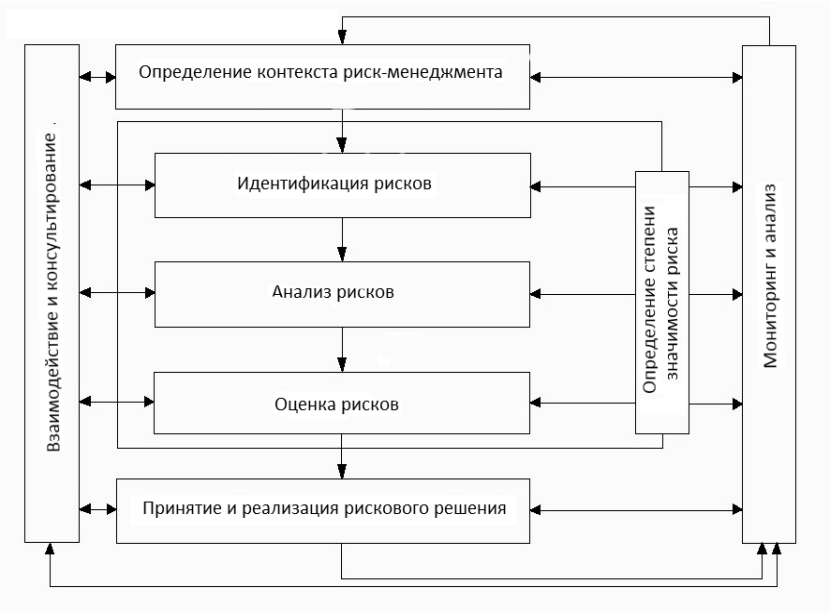


Рис. 1.3. Структурная схема процесса риск-менеджмента

Целью концепции приемлемого риска является определение оптимального компромисса между рассматриваемыми диаметрально противоположными результатами: всегда существует опасность реализации принятого управляющего решения не в полном объеме, так как невозможно устранить все причины и факторы риска, которые могут привести к появлению рисковой ситуации с негативными последствиями. В основе методологии концепции приемлемого риска лежит дифференциация уровней риска на различных стадиях его проявлений:

− начальный уровень риска Ун – уровень риска идеи, замысла или предложения без учета проведения мероприятий по анализу и оценке риска. Это риск является неидентифицированным и неоцененным и, следовательно, уровень риска на данном этапе является очень высоким вследствие неготовности менеджеров организации, принимающих решения, к появлению рисковых ситуаций;

Таблица 1.23. Характеристики основных стадий процесса риск-менеджмента

Стадия	*Характеристика*
Взаимодействие и консультирование	На каждой стадии процесса риск-менеджмента необходимо взаимодействовать и проводить консультации как с внешними, так и с внутренними участниками этого процесса
Определение контекста риск-менеджмента	Необходимо определить внешние характеристики предпринимательской среды, внутренние параметры организации, а также параметры риск-менеджмента, в которых будет реализовываться процесс. Должны быть определены требования к деятельности, на основании которых будут обнаружены критерии рисков, а также структура и методы их анализа
Идентификация рисков	Следует определить, где, когда, почему и как рисковые ситуации могут помешать, ослабить, задержать или способствовать достижению запланированных результатов (целей)
Анализ рисков	Необходимо определить последствия, вероятность возникновения и, следовательно, уровень риска, а также причины и факторы возникновения рисковых ситуаций. Подобный анализ должен учитывать масштаб потенциальных последствий и возможные пути их возникновения. При анализе рисков следует также выявить и оценить имеющиеся инструменты (модели и методы) контроля рисков
Оценка рисков	Осуществляется сравнение уровня риска с ранее установленными критериями. Согласно полученным данным и параметрам модели риск-менеджмента (см. Первую стадию) определяется баланс между потенциальными преимуществами и отрицательными последствиями. Это позволяет принимать решения о масштабе и характере рискового решения, управляющего воздействия на риск, а также устанавливать приоритетные направления деятельности, связанной с риск-менеджментом
Принятие и реализация рискового решения	Осуществляется разработка и внедрение специализированных экономически целесообразных стратегий и планов мероприятий, цель которых – увеличение потенциальной выгоды и сокращения потенциальных расходов, возникающих впоследствии рисковых ситуаций
Мониторинг и анализ	Необходимо проводить мониторинг эффективности всех этапов процесса управления рисками для постоянного улучшения деятельности.

− оцененный уровень риска Ус – уровень риска с учетом мер по идентификации, анализа и оценки риска. Размер Ус представляет собой реальную оценку уровня риска, который является риском более низкого уровня, чем Ун;

− остаточный уровень риска Уо – уровень риска с учетом разработанных и выполненных мероприятий по снижению начального уровня риска;

− конечный (приемлемый) уровень риска Ук – уровень риска, который является приемлемым с точки зрения критериев риска. Конечный уровень риска может быть равным Уо или иметь меньшее значение. В данном случае определяющим условием является разработанная система критериев риска.

С точки зрения математического моделирования концепцию приемлемого риска можно представить в виде следующих зависимостей:

$$\begin{cases} Y_{\text{Н}} \succ Y_C \succ Y_O; \\ \Delta Y = (Y_O - Y_K) \to 0; \Rightarrow Y_O = Y_K. \end{cases}$$

Полученная оценка конечного (приемлемого) уровня риска может существенно изменить мнение о «рискованности» данной деятельности. С учетом принятых мер по снижению риска его конечный уровень может оказаться приемлемым в возможной рисковой ситуации.

Рассмотренная концепция ориентирует на такие подходы к управлению риском:

− риск – это, как правило, не статический и неизменный, а управляемый параметр, на уровень которого можно и нужно делать управляющее воздействие;

− влияние можно оказать только на идентифицированный, проанализированный и оцененный риск;

− высокий уровень начального риска не должен служить априори основанием для отказа от осуществления деятельности, связанной с этим риском;

− всегда можно найти рисковое решение, обеспечивающее определенный компромисс между ожидаемой выгодой и возможными потерями.

Для практической реализация концепции приемлемого риска необходимо:

1) выявить наиболее опасные варианты решения, связанные с недостижением поставленных целей;

2) получить оценки возможного ущерба (потерь) для различных вариантов решения;

3) спланировать и осуществить мероприятия по снижению риска до приемлемого уровня;

4) проанализировать результаты деятельности и оценить затраты по управлению риском.

Таким образом, концепция приемлемого риска заключается в формировании сознательного отношения к риску. Задачами данной концепции является:

− принятие решений, основанных на анализе объективных фактов;

− разработка и осуществление мероприятий по смягчению и / или нейтрализации возможных негативных последствий в предпринимательской деятельности.

Также выделяют **консультативный подход** к пониманию сущности риск-менеджмента.

Управление рисками представляет собой не просто технический процесс, совокупность действий по формализованным алгоритмам, но и позволяет принять однозначное и детерминированное рисковое решение. Риск-менеджмент требует командной работы, которая осуществляется прежде всего в коммуникативном контексте. Взаимодействие и консультирование между участниками риск-менеджмента являются неотъемлемыми атрибутами этого процесса и должны всегда иметь открытую форму. Результативность процесса риск-менеджмента напрямую зависит от того, насколько все заинтересованные стороны будут понимать точки зрения друг друга и, при необходимости, принимать активное участие в процессе принятия решения. Консультирование является важным условием на каждой из стадий управления рисками. Вместе с взаимодействием предусматривает диалог между участниками процесса риск-менеджмента, с акцентом на консультации, а не одностороннем потоке информации от стороны, принимающей решение, к другим заинтересованным сторонам.

На стадии моделирования процессов риск-менеджмента необходимо разработать план взаимодействия его участников. Этот план должен касаться как самих рисков, так и процессов управления ими. План взаимодействия должен отражать процедуры информирования, обсуждения рисков и проведения консультаций. Внутренние и внешние коммуникации гарантируют понимание сути принятых решений и причин конкретных действий как со стороны лиц, ответственных за реализацию процессов риск-менеджмента, так и всех заинтересованных сторон. От эффективности процессов внутреннего информирования участников риск-менеджмента напрямую зависит его результативность.

Участники риск-менеджмента обычно судят о рисках на основании собственных представлений и жизненного опыта. Восприятие рисков может оказаться у разных сторон разным, причина этого кроется в различии точек зрения на события, в отличии представлений, потребностей, проблем и забот затронутых сторон в момент, когда они сталкиваются с риском или обсуждаемыми вопросами. Так как стороны могут иметь существенное влияние на принимаемые решения, важно, чтобы показатели рисков были четко определены, зафиксированы в письменном виде и включены в процесс принятия решений.

Консультативный подход:

− позволяет однозначно определить основные составляющие модели процесса риск-менеджмента;

− способствует определению адекватности идентифицированных рисков;

− сводит воедино различные области опыта при анализе рисков;

− при оценке рисков помогает правильно учесть разные точки зрения;

− позволяет правильно корректировать процесс менеджмента при обслуживании рисков.

Обеспечение заинтересованности в процессах риск-менеджмента позволяет «распределить» риски по отдельным менеджерам, а также привлечь в эти процессы всех участников риск-менеджмента. Консультативный подход помогает оценить преимущества отдельных методов контроля и необходимость одобрения и поддержки рискового решения.

В зависимости от специфики процессов риск-менеджмента, деловой культуры организации, важности и значимости рисковых ситуаций определяется необходимость и степень ведения записей (регистрации данных) на стадии взаимодействия и консультирования.

Взаимодействие в области рисков представляет собой интерактивный процесс обмена информацией и экспертными оценками основных параметров риска и управления им. Необходимо отметить, что данный процесс должен осуществляться одновременно и параллельно по двум направлениям:

- непосредственно внутри фирмы;
- между фирмой и внешними участниками риск-менеджмента.

Внутрифирменное взаимодействие должно осуществляться как по вертикальной иерархической структуре административного управления, так и с помощью линейных межфункциональных связей между структурными подразделениями фирмы.

Консультирование по своей сути является частью процесса взаимодействия и представляет собой обмен мнениями между участниками риск-менеджмента перед принятием решений или для установления приоритетов в определенном вопросе. Одним из наиболее эффективных прикладных методов использования консолидированного мнения, полученного в ходе консультаций, является метод экспертных оценок.

Консультирование имеет следующие характерные черты:

- прежде всего, это мероприятия, направленные на достижение конечного результата, а не самоцель управления рисками;
- результаты консультирования представляют собой информационную базу для принятия рисковых решений, однако они не являются управляющим воздействием на это решение.

Обмен информацией и взглядами на риски в рамках фирмы позволяет развивать коммуникационные связи внутри организации. Это помогает определять зоны особого внимания, которые требуют совместной работы и разработки общих стратегий для достижения запланированных результатов, что позволяет однозначно определить механизмы мониторинга процесса риск-менеджмента. Межфункциональное взаимодействие обеспечивает возможность диалога между простыми исполнителями, топ-менеджерами и высшим

руководством. Взаимодействие и консультации могут осуществляться на различных уровнях в зависимости от ситуации, в частности, при:

− одностороннем взаимодействия;

− предоставлении информации, например, ежегодных отчетов, информационных листков, протоколов совещаний и т.д.;

− двустороннем сотрудничестве – обмен мнениями и точками зрений между участниками риск-менеджмента.

Опыт участников риск-менеджмента в большинстве случаев является определяющим базисом, что позволяет установить причины и факторы возникновения рисковых ситуаций. Взаимодействие и консультирование способствует увеличению объективности оценки рисков и исключает «шаблонное» мышление.

Например, высшее руководство определяет направления вложения инвестиций в ряд проектов, исходя из собственных представлений о параметрах рисков. При этом топ-менеджеры организации оценивают размер риска иначе. В некоторых случаях сотрудники компании, которые функционируют на операционном уровне организации, идентифицируют ряд рисков, которые «выпали» из поля зрения их руководителей.

Таким образом, наличие обратной связи является важнейшим элементом внутреннего взаимодействия и позволяет производить эффективные модели и методы управления рисками.

Взаимодействие и консультирование является неотъемлемой частью общего процесса риск-менеджмента и должны быть реализованы на каждой стадии процесса. При управлении рисками особое значение уделяется вопросам адекватной идентификации участников риск-менеджмента, определения степени и характера их заинтересованности в конкретной стадии процесса.

На основании полученных данных разрабатывается план взаимодействия. Этот план должен установить цель взаимодействия, тех, кто и кому предоставляет консультации, когда это происходит, как происходит процесс и как он оценивается.

В организации хорошее взаимодействие является важным для разработки «культуры риск-менеджмента», различающей положительные и отрицательные аспекты риска. Взаимодействие в сфере

рисков позволяет организации разработать свою уникальную концепцию приемлемого риска.

Вовлечение в процесс риск-менеджмента других участников (например, экспертов из специализированных вопросов) или, по меньшей мере, получение экспертных оценок, является существенным и решающим фактором эффективности управления рисками. Взаимодействие с участниками риск-менеджмента делает управление рисками более взвешенными, ставит его на качественную основу и придает значимость организации.

Взаимодействие с внешними участниками риск-менеджмента гарантирует, что общие сферы интересов находятся под контролем. Такое взаимодействие увеличивает потенциал организации для установления дальнейших партнерских контактов с другими субъектами предпринимательской деятельности и для достижения положительных результатов. Так, например, внешние участники риск-менеджмента могут иметь общие риски, совместное управление которыми будет более эффективно.

В некоторых случаях организация может считать взаимодействие с участниками риск-менеджмента нецелесообразным, исходя из экономических причин и соображений безопасности. При этом план взаимодействия должен отразить осознанное решение не привлекать участников риск-менеджмента к взаимодействию, однако может в дальнейшем учитывать их точку зрения другим способом, например, в форме интеллектуальной или коммерческой информацией.

Этапы определения позиций (точек зрения на риск и его приемлемый уровень) и разработка моделей и методов взаимодействия должны быть реализованы параллельно и взаимно корреспондироваться друг в друга. При разработке планов взаимодействия необходимо учитывать позиции участников риск-менеджмента. Одна и та же рискованная ситуация будет рассматриваться заинтересованными сторонами с разных точек зрения (см. табл. 1.24) [89, 90].

Вследствие этого необходимо учитывать позиции всех участников риск-менеджмента, с тем, чтобы выработать оптимальный подход к взаимодействию и представлению информации.

Таблица 1.24. Примеры выработки методов коммуникации между основными участниками взаимодействия

№ п/п	*Группа участников*	*Определяющая точка зрения на риск*	*Метод взаимодействия и форма обмена информацией*
1	Основатели	Обеспечение получения дивидендов	Собрание учредителей, совет правления / Предоставление отчетов
2	Государственные органы исполнительной власти	Соответствие законодательным и отраслевым требованиям	Официальная переписка, совместные совещания / Предоставление отчетов о выполнении обязательных требований
3	Банковские учреждения	Гарантии возврата кредита	Деловая переписка, совместные совещания / Отчеты по платежам, данные финансовой устойчивости предприятия
4	Инвесторы	Гарантии окупаемости инвестиций	Расширенное совещание на уровне высшего руководства / Предоставление отчета о выполнении инвестиционной программы
5	Клиенты	Выполнение контрактных условий (договорных обязательств) организацией	Встречи, деловая переписка с клиентом, проведение конференций, выставок, семинаров, совместных совещаний / Предоставление отчета о ходе реализации
6	Контрагенты, поставщики, субподрядчики	Своевременность платежей по контрагентским договорам	Совместные совещания с контрагентами / Предоставление указаний контрагентам
7	Партнеры	Гарантия надежности реализации совместных проектов	Совместные совещания с партнерами / Отчетные данные по совместным проектам
8	Высшее руководство организации	Выполнение договорных обязательств перед клиентом с обязательным соблюдением бюджета и обеспечением нормы рентабельности и / или прибыли	Проведение совещаний как внутри организации, так и с участием партнеров и контрагентов / Отчеты по выполнению договора и его бюджета; оценка уровня риска в масштабах всей организации

№ п/п	*Группа участников*	*Определяющая точка зрения на риск*	*Метод взаимодействия и форма обмена информацией*
9	Топ-менеджеры	Выполнение бизнес-плана	Совещания на разных уровнях управления / Отчетные данные по реализации процессов; оценка уровня риска в рамках бизнес-процесса; варианты рискового решения, приказы
10	Менеджеры операционного уровня управления (Руководители проектов)	Обеспечение реализации процессов в управляемых условиях	Оперативные «планерки», методы «мозгового штурма» и «дельфийского оракула» / отчеты о проделанной работе; оценка уровня риска на операционном уровне управления, распоряжения
11	Ответственные исполнители по функциональному признаку	Выполнение задач, полученных от высшего уровня управления	Оперативные «планерки», методы «мозгового штурма» и «дельфийского оракула» / Отчеты о проделанной работе, служебные записки, рапорты
12	Внешние эксперты-оценщики и консультанты	Приемлемый доверительный интервал сделанных оценок и рекомендаций	Проведение совместных совещаний, методы «мозгового штурма» и «дельфийского оракула» / Предоставление отчетов о проведенных экспертных оценках уровня риска; предоставление рекомендаций по выбору вариантов рискового решения

Периодичность осуществления взаимодействия, а также объем документирования его результатов зависят от уровня управляющих решений, которые формируются в результате этого взаимодействия. Так, например, проведение совместных совещаний с инвесторами, учредителями и партнерами будет осуществляться с меньшей частотой, чем оперативные «планерки» на операционном уровне. Соответственно, совещания, которые проводятся на уровне топ-менеджмента, должны протоколироваться в обязательном по-

рядке, вместе с тем оперативные совещания далеко не всегда требуют обязательного ведения протокола.

Оценка результативности взаимодействия позволяет получить объективную картину достаточности и практической целесообразности применения выбранных методов взаимодействия. В приведенной выше таблице представлены основные методы коммуникации между участниками процесса риск-менеджмента. На разных стадиях процесса рассмотренные методы могут модифицироваться в соответствии со спецификой данной стадии.

Определение контекста риск-менеджмента

Под контекстом риск-менеджмента понимается совокупность внутренних и внешних факторов (условий), в рамках которых осуществляется управление рисками. Разработка контекста риск-менеджмента позволяет установить основные параметры (границы), в рамках которых необходимо управлять рисками. Контекст также включает в себя внутреннее и внешнее окружение компании и цель процесса риск-менеджмента. Необходимо следить за тем, чтобы цели риск-менеджмента учитывали специфику внешнего и внутреннего окружения компании.

Разработка контекста связана с определением основных идей компании, ее рисков, масштаба процесса риск-менеджмента, и с разработкой структуры задач, поставленных перед этим процессом.

Эта стадия необходима для того, чтобы:

− определить цели компании;

− определить внешние характеристики предпринимательской среды, в рамках функционирования которой необходимо достичь поставленных целей;

− конкретизировать масштаб и цели риск-менеджмента;

− определить границы процесса риск-менеджмента, а также уровень приемлемого риска;

− определить основные требования к видам деятельности компании, на которые распространяется процесс риск-менеджмента;

− определить перечень основных показателей для структурирования процесса идентификации рисков и определения их параметров.

Основной целью этой стадии является осуществление первоначальной оценки всех факторов риска, которые могут влиять на спо-

собность компании достичь запланированных целей. В результате должно получиться краткое формулирование целей организации, точных критериев успеха, целей и масштаба риск-менеджмента и последовательность этапов на стадии идентификации рисков. Особенно важно, чтобы процесс имел четкие границы (область применения, цели и задачи, входные и выходные параметры, ресурсы и управляющие воздействия), что позволит обеспечить функционирование процесса риск-менеджмента в управляемых условиях.

Как уже рассматривалось ранее, риск представляет собой соотношение вероятности возникновения рисковой ситуации и ее последствий, которое приводит к отклонению фактических результатов деятельности от запланированных. По своей сути запланированные результаты работы компании вытекают из поставленных целей – как на стратегическом уровне, так и на уровне функционирования бизнес-процессов. Поэтому, чтобы обеспечить качественную идентификацию всех значимых рисков, необходимо знать, как цели деятельности, так и цели бизнес-процессов. Определение контекста можно разбить на два основных этапа.

Первый этап определения контекста – идентифицировать цели, задачи и внутренние параметры компании, а также внешние характеристики предпринимательской среды.

Второй этап – определить масштаб процесса риск-менеджмента, основные вопросы и проблемы, которые он ставит перед организацией и взаимоотношения между стратегией организации и запланированными результатами бизнес-процессов.

При определении внешних характеристик предпринимательской среды должны учитываться следующие основные условия:

- деловое, социальное, нормативное, культурное, конкурентное, финансовое и политическое окружение организации;
- слабые и сильные стороны организации;
- перспективы компании и неблагоприятные факторы, препятствующие ее развитию;
- особенности внешних участников процесса риск-менеджмента;
- ключевые факторы экономической деятельности организации.

В ходе реализации второго этапа можно использовать основополагающие документы, такие как стратегический план, бизнес-

планы и бюджеты, годовые отчеты, экономические анализы и другую документацию, содержащую зарегистрированную информацию о деятельности организации.

Также в ходе определения контекста риск-менеджмента необходимо соотнести запланированные результаты бизнес-процессов, идентифицированные границы процесса риск-менеджмента с действующим законодательством. Установка масштаба и границ риск-менеджмента включает в себя:

− идентификацию процесса, проекта или деятельности и определение ее целей и задач;

− определение характера решений, которые необходимо принять;

− определение масштаба деятельности по проекту или функции по времени и месту;

− определение характера и масштаба необходимых исследований, их целей и ресурсов;

− определение области применения процесса риск-менеджмента, включая все исключения;

− оценку роли и ответственности различных структур организации, участвующих в процессе риск-менеджмента.

Необходимо также отметить, что процесс риск-менеджмента не будет всеобъемлющем и полным, если не определены ключевые элементы деятельности, в отношении которого осуществляется управление рисками.

Ключевые элементы деятельности представляют собой совокупность важных направлений (приоритетов деятельности), которые должны быть последовательно разработаны в процессе идентификации рисков.

Каждый ключевой элемент деятельности имеет более узкую специфику, чем вся деятельность в целом. Данное обстоятельство позволяет специалистам по идентификации рисков осуществить детальную проработку возможных причин и факторов риска.

В случае если деятельность рассматривается как единое целое, осуществить идентификацию рисков на всех этапах ее жизненного цикла крайне трудно. Тщательно разработанный набор ключевых элементов будет стимулировать творческую мысль и гарантировать полный охват всех важных тем (приоритетов деятельности).

Когда для идентификации рисков используется метод «мозгового штурма», ключевые элементы формируют повестку дня и основные задачи встречи.

В качестве практической иллюстрации этого тезиса рассмотрим следующую ситуацию.

Генподрядная строительная организация осуществляет управление строительным проектом. В рамках проекта организация выполняет также функции генерального инвестора. Непосредственно для выполнения строительно-монтажных работ привлекаются специализированные субподрядные строительные компании, прошедшие квалификационный отбор.

В табл. 1.25 [89, 90] представлены основные приоритеты деятельности, которые сформированы в результате идентификации ключевых элементов проекта. Эти приоритеты позволят в дальнейшем определить основные риски, связанные с проектом.

Данная классификация ключевых элементов и приоритетов формирует «скелет», необходимый для дальнейшей идентификации рисков. Перечень основных приоритетов деятельности указывает основные ориентиры при определении причин и факторов возникновения рисковых ситуаций.

Помимо определения ключевых элементов и приоритетов необходимо также однозначно сформулировать основные факторы ограничения. Объектом управления выступает бизнес-процесс, проект или вид деятельности, на которую распространяется управления рисками.

При определении контекста риск-менеджмента необходимо, в первую очередь, установить основные требования (ограничения) к объекту управления как деятельности.

Диапазон ограничивающих факторов может быть достаточно широким. В качестве примера представлены основные ограничения для «типичного» проекта, связанного с разработкой нового вида продукции на производственном предприятии.

Спецификация требований к проекту приведена в табл.1.26 [89, 90].

Таблица 1.25. Пример определения приоритетов деятельности при управлении строительным проектом

Ключевой элемент	*Приоритеты деятельности*
Обеспечение реализации проекта в контролируемых условиях	- Рентабельность проекта - Контроль работы субподрядчиков - Соблюдение сроков - Соответствие проекта бюджета - Контроль за соблюдением нормируемых показателей загрязнения окружающей среды - Обеспечение профессиональной безопасности
Минимизация производственных потерь	- Увеличение ликвидности и стоимости активов - Обеспечение стабильности производства строительно-монтажных работ (СМР) - Соответствие расходной части бюджета
Непрерывность производственного цикла	- Сокращение перебоев в поставках материально-технических ресурсов - Сокращение временных интервалов простоя техники - Осуществление оперативного планирования каждого этапа выполнения СМР - Ежедневная актуализация отчетов об освоении объемов накопительным итогом со стороны субподрядчиков
Управляемость и подотчетность субподрядчиков	- Анализ контрактов на субподрядные работы - Ежедневный контроль работы субподрядчиков - Технический надзор за выполнением СМР
Рентабельность проекта	- Сокращение расходов, связанных с поставками - Оптимизация величины постоянных (непроизводственных) расходов - Осуществление финансирования в рамках утвержденного бюджета проекта
Управление персоналом	- Снижение «текучести» кадров - Развитие профессиональной квалификации - Соблюдение законодательства по охране здоровья, безопасности и экологии деятельности - Сокращение рисков для здоровья, безопасности и окружающей среды при строительстве
Здоровье и безопасность работников	- Деятельность, отвечающая нормам безопасности и защиты здоровья - Сокращение рисков для здоровья и безопасности при строительстве - Отсутствие травм и смертельных случаев или длительных проблем со здоровьем
Окружающая среда	- Деятельность, отвечающая экологическим нормам и не нарушающая безопасность местного населения - Сокращение экологических рисков и рисков для местной общины во время строительства - Отсутствие выбросов в атмосферу

Идентификация рисков

Под идентификацией рисков понимаются действия, направленные на определение параметров рисковой ситуации (что может случиться, где, когда, как и почему?)

Таблица 1.26. Спецификация требований к проекту разработки нового вида продукции

Ограничения	*Пояснения*
Качество проекта	Выходные данные проекта (например, новый вид продукции) должны удовлетворять предъявляемым к ним функциональным требованиям и заданным техническим характеристикам.
Отраслевые требования	Выходные данные проекта должны соответствовать обязательным отраслевым требованиям к данному виду продукции.
Бюджет	Финансовые ресурсы, необходимые для реализации данного проекта, должны соответствовать расходной части бюджета.
Доступность ресурсов	Технологический процесс производства нового вида продукции должен быть разработан таким образом, чтобы при производстве использовалось только имеющееся промышленное оборудование и технологическая оборудование.
Экономическая целесообразность	Проект должен иметь положительное экономическое обоснование, измеряемое рентабельностью и коэффициентом окупаемости.
Сроки	Проект должен быть завершен в установленные сроки.
Обучение персонала	Реализация проекта должна способствовать росту профессионализма организации и навыков персонала.
Экология и безопасность	Технологические решения проекта должны учитывать необходимость предотвращения загрязнения окружающей среды; процессы в рамках проекта должны обеспечивать высокие стандарты профессиональной безопасности сотрудников.

Целью идентификации рисков является составление полного перечня рисков, которые могут повлиять на достижение целей организации в рамках интегрированной системы менеджмента. Этот перечень должен быть максимально полным, так как неидентифицированные риски могут представлять существенную опасность

для достижения поставленных целей, вызвать потерю контроля над процессами менеджмента рисками и привести к упущению перспективных возможностей.

Факторы риска представляют собой источник появления рисковой ситуации.

Например, нестабильность экономической ситуации в стране порождает потенциальный риск задержки погашения задолженности компании. Факторы риска – проявление интенсивности действия опасных явлений, которое при наличии уязвимостей у объекта риска приводит к возникновению рисковой ситуации.

В развитие предыдущего примера можно установить, что задержка с выплатой задолженности произошла вследствие неконтролируемого роста инфляции на фоне нестабильной макроэкономической среды на уровне государства. В данном случае фактором риска выступает неконтролируемый рост инфляции.

Рисковая ситуация представляет собой событие, обусловленное причинами и факторами риска, которые могут привести к негативным или позитивным последствиям.

Отсутствие финансирования организации со стороны дебиторской компании иллюстрирует понятие рисковой ситуации. Вид риска характеризует источник появления рисковой ситуации. Другими словами, вид риска определяет, кто из заинтересованных сторон является «инициатором» возникновения рисковой ситуации.

В рассматриваемом примере вид риска является внешним, так как его «инициатором» выступает внешняя заинтересованная сторона – дебиторская компания. Метод обнаружения характеризует способ выявления рисковой ситуации. Отсутствие финансирования оказывается финансово-экономической службой организации путем мониторинга расчетного счета договорных обязательств между организацией и дебитором. Характеристики рисковой ситуации определяются временными и структурными параметрами появления риска.

В нашем примере отсутствие финансирования может возникнуть на этапе выполнения дебитором своих обязательств. Последствия представляют собой результаты рисковой ситуации в случае их реализации. Рассмотренная рисковая ситуация ведет к негативным последствиям для организации, например, к срыву временных

характеристик (сроков) при реализации бизнес-процесса или проекта. Разработать всеобъемлющий перечень рисков можно в рамках систематического процесса управления рисками, который необходимо начинать с формулировки и определения контекста риск-менеджмента (см. п. 1.3). Для обеспечения гарантии результативности идентификации рисков рекомендуется подходить к исследованию бизнес-процесса, проекта или деятельности путем их последовательного структурирования. Базовый алгоритм разработки такой процедуры представляет собой ряд последовательных вопросов. Ответы на них позволяют разработать эффективную процедуру идентификации рисков. Уровень детализации вопросов зависит от статуса процесса риск-менеджмента в контексте деятельности, на которую он распространяется.

Идентификация рисков является одним из базовых и основных элементов риск-менеджмента. При идентификации рисков определяющим фактором является качество исходной информации. Качество информации определяется следующими основными параметрами:

- подлинность;
- объективность;
- своевременность;
- актуальность;
- полнота охвата.

При идентификации рисков рекомендуется использовать метод «мозгового штурма» и метод экспертных оценок. Можно выделить следующие источники получения информации, используемой при идентификации рисков:

- проведение консультаций с группами специалистов, имеющих опыт в реализации деятельности, в рамках которой осуществляется управление рисками;
- опыт конкурентов и других сторонних организаций;
- SWOT-анализ и результаты маркетинговых исследований;
- отчеты по страховым случаям;
- результаты внутренних и внешних аудитов;
- результаты инспекционных проверок технологии реализации бизнес-процессов;

− записи прошлых событий, базы данных по событиям, анализ проблем и предыдущие перечни рисков (если таковые имеются).

При идентификации рисков необходимо также определиться со схемой их классификации. Классификация рисков позволяет разделить их на однородные кластеры, дает возможность систематизировать риски. Необходимость классификации связана с тем, что основной причиной возникновения рисковой ситуации является неопределенность предпринимательской среды – как внутренней, так и внешней. Классифицировать риски можно по различным признакам. При этом необходимо стараться не столько перечислить все виды рисков, сколько создать определенную базовую схему, которая позволила бы не упустить какие-либо из них.

Стандарт ISO/FDIS 31000

Стандарт ISO/FDIS 31000 [74] (Risk management – Principles and guidelines (Управление рисками – руководящие принципы), Швейцария) описывает основные принципы АОР. В нем определены 7 основных этапов управления рисками:

1. Описание структуры организации и ее контекста;
2. Определение политики риск-менеджмента. Политика должна четко отображать цели организации;
3. Определение ответственности;
4. Интеграция в организационные процессы;
5. Идентификация ресурсов;
6. Создание внутренних связей и механизмов отчетности;
7. Создание внешних связей и механизмов отчетности организации.

Для проведения АОР определяются критерии риска, которые должны отразить цели и ресурсы организации, быть совместимыми с ее политикой риск-менеджмента, определенны в начале любого процесса риск-менеджмента и постоянно пересматриваться. Далее переходят к процессу оценке степени риска – полный процесс его идентификации, анализа и оценки. На этапе анализа определяются последствия, вероятность и другие признаки риска [74, 87, 91, 92].

В течение последней четверти века ведущими разработчиками стандартов по риск-менеджменту считались канадская, австралийская и японская национальные ассоциации стандартов, Междуна-

родная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC, укр. – МЭК), Австрийский институт стандартов, др. Длительное и тщательное исследование международных и национальных стандартов управления рисками, выполненное в начале XXI века, указало на существование достаточно существенного расхождения в трактовке основных понятий в ряде действующих стандартов, в частности в подходах к идентификации внешних и внутренних рисков и, соответственно, построения организационных схем процесса риск-менеджмента. Для решения данной проблемы Международная организация по стандартизации инициировала разработку международного стандарта управления рисками ISO 31000: 2009 – Risk management – Principles and guidelines (Управление рисками. Принципы и рекомендации).

При подготовке данного стандарта за основу было взято Австралийско-Новозеландский стандарт AS/NZS 4360:2004 (это объясняет, почему оба стандарта, AS/NZS 4360:2004 и ISO 31000: 2009, равно определяют и описывают процесс риск-менеджмента и его отдельные составляющие).

Работа над стандартом ISO 31000:2009 была начата в 2005г. В разработке данного стандарта приняли участие эксперты из 28 стран и многих специализированных организаций [93].

При разработке ISO 31000: 2009 были учтены недостатки предыдущих стандартов риск-менеджмента. В ноябре 2009 данный стандарт был официально опубликован. В общем, стандарт ISO 31000: 2009 должен обеспечивать поддержку имеющимся принятым ранее стандартам по управлению рисками, которые используют в определенных направлениях (безопасность транспорта, профессиональное здоровье и безопасность, экология, медицина, энергетика и т.п.). ISO 31000: 2009, по сути, является документом, который может помочь организациям разработать собственные подходы к управлению рисками. Внедряя данный стандарт, организация может сравнить свою практику управления рисками с международным опытом и поделиться собственным. Кроме того, необходимо подчеркнуть, что стандарт ISO 31000: 2009 был разработан для помощи организациям в следующем [94]:

- повысить вероятность достижения целей;
- стимулировать предупредительное управления;

− осознать необходимость в идентификации и оценке рисков всей организации;

− улучшить процесс идентификации возможностей и угроз;

− отвечать организационным, законодательным и нормативным требованиям и международным нормам;

− улучшить регулярную отчетность;

− усовершенствовать управление;

− увеличить доверие заинтересованных лиц (акционеров, инвесторов и т.д.);

− создать надежную основу для принятия решений и планирования;

− усовершенствовать методы управления;

− эффективно распределять и использовать ресурсы для управления рисками;

− улучшить операционную результативность и эффективность;

− повысить результативность мер, направленных на защиту здоровья, безопасности и окружающей среды;

− усовершенствовать подходы по предупреждению потерь и управления инцидентами;

− минимизировать убытки;

− усовершенствовать обучение персонала;

− обеспечить устойчивость организации.

Важным дополнительным элементом стандарта ISO 31000: 2009 является «Справочник ISO 73: 2009», содержащий словарь риск-менеджмента. Данный словарь – это обновленный словарь по риск-менеджменту ISO/IEC, являющийся частью Справочника 73: 2002. Фактически, этот справочник – основной стандарт для разработчиков стандартов по риск-менеджменту. А новый словарь должен решить проблему, которая заключается в том, что в разных стандартах управления рисками по-разному определяют и объясняют основные понятия риск-менеджмента. Однако адаптация к терминологии стандарта ISO 31000: 2009 при наличии системы управления рисками, основанной на стандартах, очень отличающихся от упомянутого стандарта, потребует значительных усилий и даже полного изменения системы управления рисками [95]. Это объясняется тем, что в разных стандартах риск-менеджмента по-разному определяют даже понятия риска. В международном стандарте

ISO 31000: 2009 риск истолкован как влияние неопределенности на обработанное задание. Согласно данному документу, риск – это следствие постановки и достижения организационных задач при неопределенности окружающей среды. Соответственно, неопределенность порождается внешними и внутренними факторами, которые организация не может полностью контролировать и которые могут негативно повлиять на выполнение задания или отсрочить его. Указанные факторы и их влияние могут также способствовать заблаговременному и успешному достижению цели. Соответственно, риск не является отрицательным или положительным явлением, однако его последствия могут иметь негативное или положительное значение для организации. Итак, в стандарте ISO 31000: 2009 упор в определении риска смещается от вероятности события (что-то может произойти) к вероятности последствия, особенно его влияния на выполнение определенных задач. До данного стандарта риск определялся как негативное явление, которого организация пытается избежать или передать другим. Сегодня специалисты понимают, что риск является частью жизни, он может быть не только отрицательным.

Как уже было отмечено, за основу международного стандарта ISO 31000: 2009 взято Австралийско-Новозеландский стандарт AS / NZS 4360: 2004, поэтому и процесс управления рисками в обоих стандартах очень похож. Процесс управления рисками ISO 31000: 2009 отражено на рис. 1.4.

Согласно стандарту ISO 31000: 2009 процесс управления рисками начинается с определения целей, которые организация хочет достичь, а также внутренних и внешних факторов, которые могут повлиять на достижение намеченных задач. Данный этап называется «Определение окружения» (establish the context), он предшествует этапу идентификации рисков.

Оценка риска в соответствии с ISO 31000: 2009 состоит из трех этапов: 1 этап – идентификация; 2 этап – анализ; 3 этап – непосредственная оценка. Процесс оценки риска должен быть систематическим. Только при таких условиях можно понять, что может произойти, как, когда и почему. В стандарте ISO 31000: 2009 этап анализа риска связан с развитием понимания каждого риска, его последствий и вероятностей этих последствий.

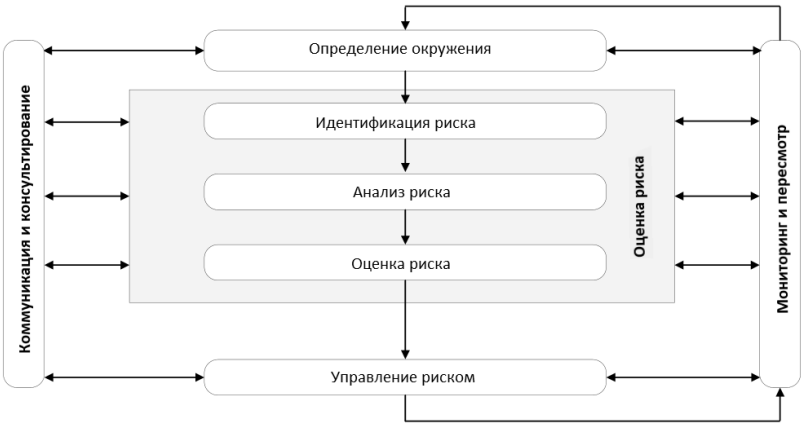


Рис. 1.4. Структурная схема процесса риск-менеджмента по стандарту ISO 31000: 2009

Стандарт ISO 31000: 2009 не дает преимущества количественным или качественным методам анализа риска, поскольку, по мнению разработчиков, все методы являются важными. После оценки риска принимают решение по определению уровня риска и по предварительно установленным критериям определяют приоритетные риски. Этап управления рисками – это процесс совершенствования имеющихся, а также разработка и внедрение новых методов управления рисками. Управление рисками охватывает оценку и выбор альтернатив развития рисковой ситуации, а также анализ затрат и преимуществ и оценку новых рисков, которые могут быть вызваны выбором того или иного метода управления рисками.

Данным стандартом могут пользоваться государственные, частные, общественные организации или предприятия и ассоциации. ISO 31000: 2009 не является специальным стандартом для определенной отрасли или сектора. Этот стандарт можно использовать для формирования / совершенствования интегрированной системы управления рисками. Специалисты по риск-менеджменту считают, что по сравнению со стандартом управления рисками, который разработал Комитет организации-спонсоров комиссии Тредвея (COSO), стандарт ISO 31000: 2009 имеет ряд преимуществ при

совершенствовании или формировании интегрированной системы управления рисками.

Применение проанализированных стандартов риск-менеджмента позволяет: оценить меры по управлению рисками, выявить слабые и сильные аспекты корпоративного риск-менеджмента, снизить затраты на подготовку соответствующих отчетов, внести необходимые изменения в организационную структуру, повысить эффективность организации и тому подобное. Необходимо подчеркнуть, что международный стандарт ISO 31000: 2009 можно активно использовать и при разработке национальных стандартов управления рисками [74].

Область применения

Стандарт ISO 31000: 2009 устанавливает принципы и содержит общие руководящие указания по менеджменту риска. Стандарт можно применять к любому типу риска, независимо от его характера, а также негативных или позитивных последствий.

Несмотря на то, что стандарт предоставляет общие руководящие указания, он не предназначен для обеспечения одинакового менеджмента риска во всех организациях. При создании и применении планов и структуры менеджмента риска необходимо учитывать различные потребности конкретной организации, цели ее функционирования, контекст, структуру, деятельность, процессы, функции, проекты, продукцию, услуги или активы и конкретные используемые практические методы. Настоящий стандарт не предназначен для целей сертификации.

Принципы менеджмента риска организации

Эффективный менеджмент риска организации на всех уровнях отвечает таким принципам:

1) создает и обеспечивает ценности;

2) является неотъемлемой частью всех организационных процессов;

3) является частью принятия решения;

4) подробно рассматривает и анализирует любые неопределенности;

5) является систематическим, структурированным и своевременным;

6) основывается на соответствующей доступной информации;

7) является целенаправленным;

8) учитывает человеческие и культурные факторы;

9) является прозрачным и всесторонним;

10) является динамичным, повторяющимся и измеряемым;

11) способствует постоянному улучшению качества функционирования организации.

Структура менеджмента риска

Общие положения

Применение менеджмента риска будет зависеть от эффективности структуры менеджмента, обеспечивающей основу и мероприятия, которые должны применяться в организации на всех уровнях. Структура способствует эффективному менеджменту риска посредством применения процесса менеджмента риска на разных уровнях и в рамках конкретных контекстов организации. Структура гарантирует, что информация о риске, полученная в процессе менеджмента риска, соответствующим образом документируется и используется в качестве основы для принятия решений и отчетности на всех соответствующих уровнях организации.

Полномочия и обязательства

Внедрение менеджмента риска и обеспечение его постоянной эффективности требует принятия обязательств со стороны руководства организации, а также стратегического и оперативного планирования для выполнения обязательств на всех уровнях.

Разработка структуры менеджмента риска

Основными факторами, обеспечивающими удачное формирования структуры проведения процедуры менеджмента риска, являются:

- понимание организации и ее контекста;
- определение политики менеджмента риска;
- ответственность;
- интеграция в организационные процессы;
- ресурсы;
- установление внутренних механизмов обмена информацией и отчетности;
- установление внешних механизмов обмена информацией и отчетности.

Процесс менеджмента риска организации

В общем случае процесс менеджмента риска состоит из ряда типовых этапов. Ниже приведена их последовательность и краткое содержание некоторых.

1) Сбор необходимой информации.

2) Обмен информацией и консультирование.

Обмен информацией и консультирование с внешними и внутренними заинтересованными сторонами осуществляются на всех этапах процесса менеджмента риска, поэтому планы по обмену информацией и консультированию должны разрабатываться на ранних этапах. В ходе обмена информацией и консультирования должны рассматриваться вопросы, касающиеся самого риска, его причин, его последствий (если известны) и мер, принимаемых для обработки риска.

3) Установление окружения (выяснения контекста, определение критериев риска).

В процессе реализации информационно-аналитических мероприятий, связанных с выяснением контекста функционирования организации, формулируются цели организации, определяются внешние и внутренние параметры, которые следует принимать во внимание при осуществлении менеджмента риска, а также определяется область применения и критерии риска для процесса менеджмента риска. Непосредственно в процедуре определения контекста выделяются три составляющие:

- установление внешнего контекста;
- установление внутреннего контекста;
- установление контекста процесса менеджмента риска.

Определение контекста осуществляется к цели, стратегии, области применения и параметрам деятельности организации в целом или только тех ее частей, где применяется процесс менеджмента риска.

Обязательным элементом процесса менеджмента риска организации является определение критериев, которые необходимо использовать для оценки значимости риска. Критерии должны отражать ценности, цели и ресурсы организации. Некоторые критерии могут устанавливаться на основе законодательных и обязательных требований, а также других требований, которые взяла на себя организация.

4) Оценка риска.

Оценка риска – это целостный комплексный процесс, который сочетает в себе этапы идентификации риска, анализа риска и аттестации риска. Рассмотрим содержание каждого из этапов.

5) Идентификация риска.

Цель данного этапа заключается в составлении подробного перечня рисков, основанного на тех событиях, которые могут создавать, повышать, предотвращать, снижать, ускорять или замедлять достижения целей и мешать нормальному функционированию организации.

6) Анализ риска.

Анализ риска обеспечивает понимание риска, предоставляет исходные данные для оценки риска (в частности, оценочные значения вероятностей и убытков, необходимых для вычисления количественных оценок рисков) и принятие решений по обработке рисков, а также для выбора стратегий и методов наиболее подходящей обработки рисков.

7) Непосредственная оценка (аттестации риска).

Целью аттестации риска является помощь в принятии решений, основанных на результатах анализа риска относительно необходимости обработки рисков и установления приоритетов осуществления обработки риска.

8) Управление риском.

Управление риском включает выбор одного или нескольких вариантов изменения (уменьшения, предотвращения, исключения) рисков и применение этих вариантов.

9) Выбор вариантов обработки риска.

Выбор наиболее подходящего варианта обработки риска включает сопоставление затрат и усилий по реализации изменений риска с полученными результатами (с учетом законодательных, обязательных и других требований, в частности таких, как социальная ответственность и защита окружающей среды).

10) Подготовка и реализация планов обработки риска.

Целью планов обработки риска является документирование того, как должны реализовываться выбранные варианты обработки.

11) Мониторинг и анализ.

Мониторинг и анализ действий менеджмента риска должны быть планируемой частью процесса менеджмента и включать регулярную проверку или контроль. Они могут быть периодическими или специальными.

12) Документирование процесса менеджмента риска.

Деятельность по менеджменту риска должна быть четко очерчена и зафиксирована. В процессе менеджмента риска записи обеспечивают основу для улучшения методов и инструментов, а также всего процесса менеджмента.

Все организации должны достичь соответствующего уровня функционирования структуры менеджмента рисков в соответствии с важностью решений, которые должны быть приняты.

Международный стандарт ISO/IEC 31010

Этот стандарт разработан в дополнение к ISO/IEC 31000 и содержит рекомендации по выбору и применению методов оценки риска. Оценка риска, определенная в соответствии с этим стандартом, применима при выполнении других элементов процесса менеджмента риска. В настоящем стандарте представлены методы оценки риска и приведены ссылки на другие международные стандарты, в которых более подробно описано применение конкретных методов оценки риска.

Этот стандарт не предназначен для установления соответствия качества полученных решений и совокупности сформулированных обязательных или договорных требований. Стандарт не содержит конкретных критериев для принятия решения по анализу риска и указаний по применению методов анализа риска в конкретной ситуации.

Этот стандарт предполагает использование других (не описанных или не определенных в нем) методов оценки риска с учетом их применения в конкретной ситуации. Данный стандарт не связан с аспектами безопасности.

Стандарт является основополагающим стандартом в области менеджмента риска, и любые ссылки на безопасность носят справочный характер. При введении в действие требований безопасности следует руководствоваться положениями соответствующих международных стандартов.

Основные понятия оценки рисков

Основной целью оценки риска является представление на основе объективных сведений информации, необходимой для принятия обоснованного решения относительно способов обработки риска.

Оценка риска, приведенная в настоящем стандарте, соответствует структуре и процессу менеджмента риска, установленным стандартом ISO 31000. Структура менеджмента риска организации предполагает установление политики, процедуры и организационных мероприятий, направленных на внедрение менеджмента риска во всех подразделениях организации.

Оценка риска является основным элементом процесса менеджмента риска организации и включает, в соответствии с ISO 31000, следующие элементы:

- обмен информацией (коммуникацию) и консультации;
- установление области применения менеджмента риска;
- оценивание риска (включая идентификацию риска, анализ риска и сравнительную оценку риска);
- обработку риска;
- мониторинг и анализ риска.

Идентификация риска – это процесс определения элементов риска, составление их перечня и описания каждого из элементов риска. Целью идентификации риска является составление перечня источников риска и событий, которые могут повлиять на достижение каждой из установленных целей организации или сделать выполнение этих целей невозможным.

Анализ риска включает в себя изучение, исследование и верификацию информации о риске. Анализ риска обеспечивает входные данные процесса формирования общей оценки риска, помогает в принятии решений о необходимости обработки риска, а также помогает выбрать соответствующие стратегии и методы обработки риска.

Сравнительная оценка риска заключается в сопоставлении уровня риска с критериями риска, установленными при определении области применения менеджмента риска для определения типа риска и его значимости.

Процесс оценки риска должен быть документированным, т.е. должна быть зарегистрирована выполненная последовательность

действий вместе с полученными результатами и оценками. Риск должен быть выражен в понятных и точных терминах и единицах.

Выбор методов оценивания риска

Оценивание риска может быть выполнено с различной степенью глубины и детализации, с использованием одного или нескольких методов различного уровня сложности. Форма оценивания и ее выходные данные должны быть совместимы с критериями риска, установленными при определении сферы применения.

При выборе метода оценки риска необходимо учитывать, что метод должен:

− отвечать рассматриваемой ситуации и организации – ОР;

− предоставлять результаты в форме, которая способствует повышению осведомленности о виде риска и способах его обработки;

− обеспечивать прослеживаемость, воспроизводимость и верификацию процесса оценки риска и полученных в ходе его результатов.

После принятия решения о выполнении оценки риска и определение сферы применения полученных оценок, следует выбрать методы оценки риска с учетом:

− цели исследования: цели оценки риска непосредственно связаны с методами, которые используются для достижения этих целей;

− ответственности принятых решений: в некоторых случаях для того, чтобы принять решение, необходим высокий уровень детализации знаний и сведений о механизме функционирования, состояние и параметры ОР, в других – достаточно более общего понимания о характеристиках и определенных особенностях ОР;

− типа и диапазона анализируемого риска;

− возможных последствий опасного события: решение относительно глубины оценки риска должно отражать первоначальное восприятие последствий (которое, скорее всего, изменится после завершения предварительной оценки риска);

− степени глубины необходимых экспертиз человеческих и других ресурсов. Простой и правильно примененный метод, в случае, если он соответствует области применения оценки, может обеспечить лучшие результаты, чем сложная процедура,

выполненная с ошибками. Обычно усилия по оценке риска должны соответствовать уровню риска, который составляет предмет анализа;

− доступности информации и данных: для некоторых методов необходимо больше информации и данных, чем для других;

− потребности в модификации или обновлении оценки риска: скорее всего, в будущем оценка должна быть изменена или обновлена, и для этого могут быть применены различные методы;

− обязательных и договорных требований.

На выбор метода оценивания риска влияют различные факторы, такие как доступность ресурсов, характер и степень неопределенности данных и информации, сложность метода.

В частности, если речь идет о факторах доступности ресурсов, во внимание следует принимать следующее:

− практический опыт, навыки и возможности группы оценки риска;

− ограничения по времени и другие ресурсы организации;

− доступный бюджет (в случае необходимости дополнительного привлечения внешних ресурсов).

Характер и степень неопределенности информации включают в себя понимание качества, количества и полноты информации о рисках, которые должны анализироваться. Понимание включает в себя осознание достаточности полученной информации о риске, его источники и причины, его последствия для достижения установленных целей.

Неопределенность может быть связана с неопределенностью данных, их неполнотой или недостоверностью.

Задача оценки риска может быть комплексной, например, оценка риска для сложной системы не сводится к раздельному определению оценок отдельных рисков ее компонентов без учета их взаимодействия.

Необходимо понимать связь последовательности действий и рисков, чтобы избежать ситуации, при которой действия по управлению одним риском приводят к катастрофической ситуации с рисками в другой части сложной системы.

1.6. Методы и средства анализа и оценивания рисков

По аналогии с п. 1.5 осуществим анализ входных, внутренних и выходных параметров, которые используются для АОР в подобных методах и средствах.

Метод CRAMM

Метод CRAMM (CCTA Risk Analysis and Management Method, разработчик – CCTA, Великобритания**)** реализован фирмой Insight Consulting Limited в одноимённом программном продукте [96]. Здесь оценивание реализуется в три этапа.

На первом – проводится идентификация физических, программных и информационных ресурсов, содержащихся внутри границ системы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Для данных и программного обеспечения (ПО) выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

Например, шкала оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов» отображается через следующие значения [96, 97]:

- 2 балла – менее $1000;
- 6 баллов – от $1000 до $10 000;
- 10 баллов – свыше $100 000 и т.д.

На втором этапе рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей.

Программное средство CRAMM для каждой группы ресурсов (и каждого из 36 типов угроз) генерирует список запросов, для которых после инициализации данных оценка уровней осуществляется, например, как очень высокий, высокий, средний, низкий, очень низкий (для угрозы), и как высокий, средний и низкий (для уязвимости).

Угрозы и уязвимости объединяются в матрице риска, а для создания шкал, например, используются данные из табл. 1.27.

Анализ риска проводится на первом и втором этапах, после чего осуществляется его оценка.

Во время анализа предлагается проставить коэффициенты для каждого ресурса с точки зрения частоты возникновения угрозы и вероятности реализации угрозы. Исходя из оценок стоимости ресурсов защищаемой ИС, угроз и уязвимостей, определяются «ожидаемые годовые потери».

Таблица 1.27. Шкалы для уровней угроз и уязвимостей

Шкалы	Описание	Значение
Шкала оценки уровней угрозы (частота возникновения)	Инцидент происходит в среднем, не чаще, чем каждые 10 лет	очень низкий
	Инцидент происходит в среднем один раз в 3 года	низкий
	Инцидент происходит в среднем раз в год	средний
	Инцидент происходит в среднем один раз в четыре месяца	высокий
	Инцидент происходит в среднем раз в месяц	очень высокий
Шкала оценки уровня уязвимости (вероятность успешной реализации угрозы)	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	низкий
	В случае возникновения инцидента, вероятность развития событий по наихудшему в пределах от 0,33 до 0,66	средний
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию выше 0,66	высокий

Рассмотрим пример матрицы оценки ожидаемых потерь [97] (рис 1.5, а), где второй столбец слева содержит значения стоимости ресурса при этом используется денежная шкала (рис. 1.5, б), верхняя строка заголовка таблицы – оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка – оценку вероятности успеха реализации угрозы (уровня уязвимости).

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

а)

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

б)

Рис. 1.5. Пример работы системы:
а) матрица ожидаемых годовых потерь; б) шкала оценки.

Значения ожидаемых годовых потерь (Annual Loss of Expectancy) переводятся в баллы, показывающие УР, согласно шкалы, представленной на рис. 1.5, б) (в этом примере размер потерь приводится в фунтах стерлингах) и далее в соответствии с матрицей (рис. 1.6) выводится ОР.

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 1.6. Матрица ОР

Третий этап реализует поиск адекватных контрмер. Здесь CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. ОУ и уязвимостей осуществляется на основе ОР по двум факторам – риск рассматривается как комбинация вероятности реализации угрозы и уязвимости, а также ущерба [87, 96-99].

Метод на основе байесовских сетей (МБС)

Метод МБС [99] разработан для построения каузальных моделей оценки операционных рисков. В его основе лежит теорема Байеса, ценность которой применительно к оценке таких рисков заключается в её способности комбинировать данные о вероятности

событий, получаемых экспертным и статистическим путём. Каждому связанному с риском событию (например – «Хакерская атака», «НСД», «НСМ» и др.), проводится оценка вероятности его реализации и (по цепочке) связанных с ним операционных потерь.

Вероятность реализации события может быть указана в виде непрерывной функции распределения или в виде таблицы вероятностей (дискретных вероятностей). Пример экспертного задания условной вероятности показан в табл. 1.28 [99]. Определяется абсолютная вероятность и величина расходов.

Рассматриваются три категории последствий: нарушение конфиденциальности (К), целостности (Ц) и доступности (Д). Для материальных активов ущерб определяется по шкале – от полной утраты актива до сбоя (остановки, неполадки) на несущественный промежуток времени [98, 99].

Таблица 1.28. Формирование вероятности

	Исходы - условия			
Хакерская атака	ДА		НЕТ	
Заражение вирусом	Да	Нет	Да	Нет
Вероятность исхода события «Остановка сервера» для различных условий				
Произойдет	0,3	0,15	0,10	0,02
Не произойдет	0,7	0,85	0,90	0,98

Метод VAR

Метод VAR [100] (Value at Risk) основан на статистическом подходе и позволяет оценить риск в терминах возможных потерь, соотнесенных с их ВВ [100]. Здесь описывается квантиль прогнозируемого распределение потерь в течение определенного периода времени.

Процесс оценивания включает этапы: идентификацию угроз, оценки их вероятности, вычисление ценности с учетом опасности и уменьшение риска. Изначально реализуется классификация угроз, таких как, например, мошенничество, злонамеренные действия, шутки, попытки получить доступ к частной информации, стихийные бедствия, саботаж, ошибки пользователей и др. Когда угрозы были идентифицированы, их вероятность (распределение вероят-

ности) оценена, возможные сценарии описаны, то определяется опасность для фирмы при реализации угроз [87, 100].

Методика COBRA

Методика COBRA (Consultative Objective and Bi-Functional Risk Analysis, разработчик – C & A Systems Security Ltd**,** Великобритания) ориентирована на поддержку требований стандарта ISO 17799 посредством тематических вопросников (check list's) [101].

В комплект ПО входят модули COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а также менеджер модуля COBRA, используемый для настройки и изменения снабжаемой базы знаний.

На основе инициализации тематического вопросника (ТВ) осуществляется АОР по следующим категориям:

- высокоуровневая;
- IT безопасности;
- оперативная IT и бизнеса;
- инфраструктуры электронной коммерции.

Модули ТВ информационно поддерживают отдельные приложения, например:

- APP-MAN (Application level security management) – управления безопасностью;
- APPAUDIT (Application level Auditing) – аудит;
- APPCNTRL (Application Staff control) – контроль штата;
- APPDEPND (Application Staff dependency) – зависимость штата;
- AUDIT (System Audit) – проверка системы и т.д.

После обработки инициализированных данных система генерирует отчет, в котором описана детальная оценка (Detailed Risk Assessment (continued)) по следующим характеристикам риска:

- категория (RISK CATEGORY);
- уровень (RISK LEVEL);
- оценка (RISK ASSESSMENT).

Отметим, что в анализируемой методике риск отображается тремя характеристиками, первая и последняя из которых несут в себе идентифицирующую составляющую (название категории и комментарии к ней), а оставшаяся – оценочную составляющую,

которой соответствует «УРОВЕНЬ РИСКА», представленный в процентах (вероятность наступления риска).

Анализ и ОР происходит во время обработки данных, инициируемых через ТВ. Все рассматриваемые действия, которые отображаются в запросах, интегрированные в категории риска, например, действие, рассмотренное в примере запроса, входит в категорию риска «Непредвиденная ситуация в бизнесе (НСБ)».

После описания всех категорий и ранжирования уровней риска (с самого высокого до нулевого) в методике приводятся рекомендуемые меры по их снижению.

Метод Coras

Метод Coras (разработан в рамках программы Information Society Technologies Европейского союза (SINTEF ICT, Норвегия) используется для анализа рисков безопасности критически важных систем и реализуется посредством технологии UML (Unified Modeling Language – унифицированный язык моделирования). Метод ориентирован на поддержку требований стандартов AS/NZS 4360: 1999 (Risk Management) и ISO/IEC 17799-1: 2000 (Code of Practice for Information Security Management).

Средство оценивания (метод) основывается на восьми шагах [102] (см. рис. 1.7).

Шаг 1 – сбор общей информации об объекте анализа.

Шаг 2 – определение цели, направления и масштаба анализа.

Шаг 3 – детализация задач анализа (см. рис. 1.8).

Шаг 4 – анализ и изучение полученной документации.

Шаг 5 – определение рисков на основе метода «мозгового штурма».

Шаг 6 – определение уровня рисков, оценивание вероятностей для угроз (сценариев угроз) и последствий инцидентов ИБ (см. рис. 1.9).

Шаг 7 – определение приемлемых и неприемлемых рисков.

Шаг 8 – определение процедур для устранения угроз с целью уменьшения возможной вероятности (последствий инцидентов) в области ИБ.

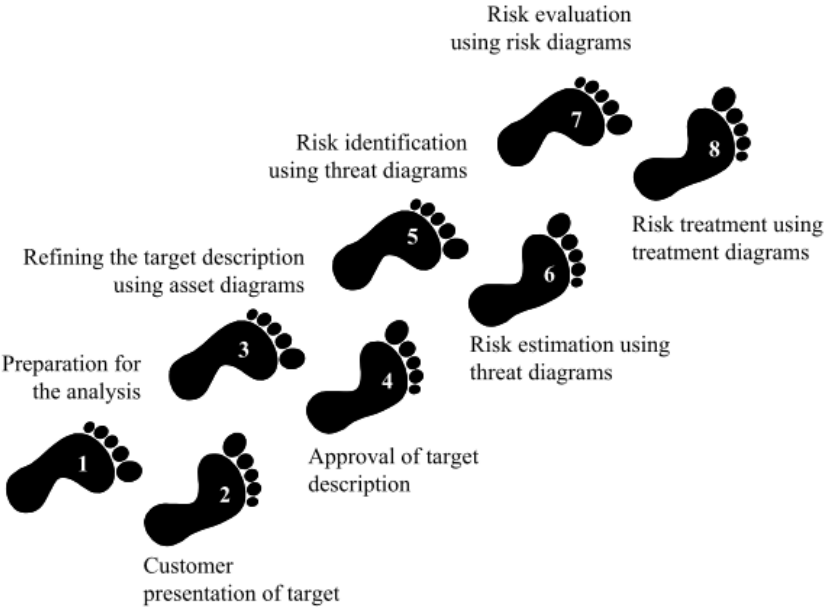


Рис. 1.7. Восемь шагов метода Coras

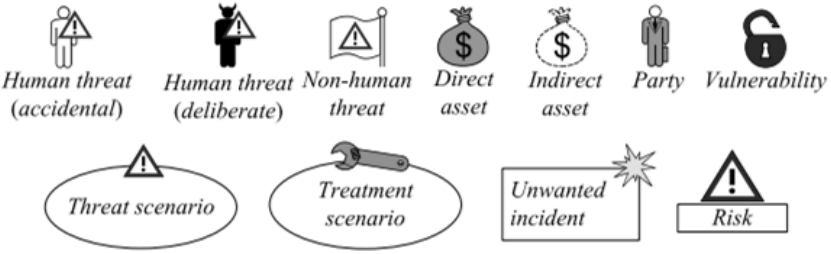


Рис. 1.8. Примеры символов для моделирования риска

Шаги 1-4 являются подготовительными, поскольку здесь аналитики собирают информацию об объекте анализа, формируют его цели и шкалы для определения величины вероятности и последствий (см. табл. 1.29 и 1.30), а также критерии оценивания рисков (см. табл. 1.31).

Таблица 1.29. Пример вероятностной шкалы

Значение вероятности	Описание	Определение
Точно	Пять и более раз в год	[50; ∞〉 : 10 лет = [5; ∞ 〉 : 1 год
Вероятно	От двух до пяти раз в год	[20; 50〉 : 10 лет = [2; 5〉 : 1 год
Возможно	Менее чем 2 раза в год	[5; 20〉 : 10 лет = [0,5; 2〉 : 1 год
Вряд ли	Меньше чем 1 раз в 2 года	[1; 5〉 : 10 лет = [0,1; 0,5〉 : 1 год
Редко	Меньше чем 1 раз в 10 лет	[0; 1〉 : 10 лет = [0; 0,1〉 : 1 год

Далее это будет использоваться для идентификации последних.

Шаги 5-8 предназначены для анализа и непосредственно определения рисков, их уровней (см. табл. 1.31), выявления и оценивания потенциальных возможностей уменьшения неприемлемых рисков [102].

Таблица 1.30. Пример шкалы последствий

Значение последствия	Количество ресурсов*
Катастрофическое	>1000
Большое	101÷1000
Среднее	11÷100
Низкое	1÷10
Незначительное	0
*ресурсы, подвергающиеся воздействию	

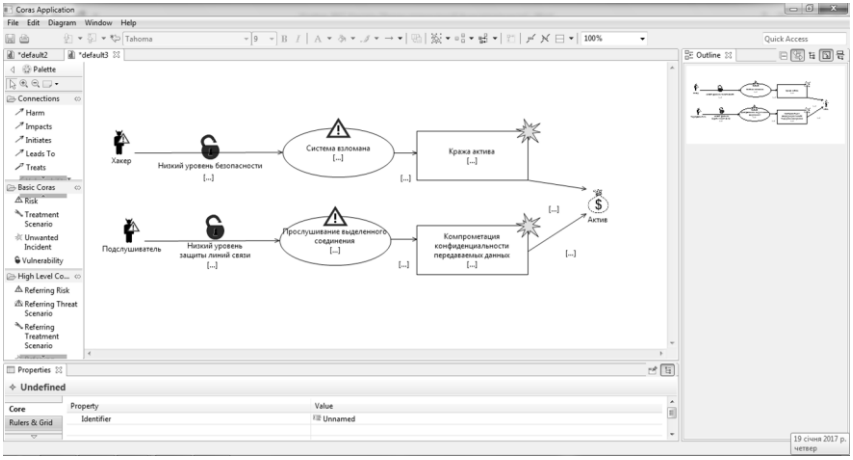


Рис. 1.9. Пример интерфейса инструментария Coras
(первоначальная схема угроз для умышленных действий)

Таблица 1.31. Пример матрицы оценки риска

Вероятность	Последствие				
	Незначительное	Низкое	Средние	Большое	Катастрофическое
Редко			CC1, CC1(I)		
Вряд ли					PR1
Возможно		CI1(I), SS1(I)	CI1, SS1		
Вероятно				SS2	
Точно					

CC1, CC1(I) – компрометация конфиденциальности, а (I) показывает, что ресурс косвенный; CI1, CI1(I) – компрометация целостности; SS1, SS1(I) – замедление системы; SS2 – невозможность работать из-за зависания системы; PR1 – получения неправильных данных.

Метод EBIOS

Метод EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, разработчик Национальное агентство компьютерной безопасности (ANSSI), Центральное управление безопасности информационных систем (DCSSI), Франция) отображает требования стандартов ISO/IEC 27001 [1, 103], ISO 31000 [74] и ISO/IEC 27005 [84]. Процесс анализа и оценивания риска реализуется посредством пяти модулей.

Модуль 1 – исследование контекста. Здесь реализуется сбор информации об объекте оценивания посредством трех мероприятий.

Мероприятие 1 – определение сферы управления рисками.

Мероприятие 2 – подготовка метрик (критерии безопасности (табл. 1.32), уровни опасности (табл. 1.33) и вероятности (табл. 1.34) и критерии управления рисками).

Мероприятие 3 – идентификация РИС [104].

Модуль 2 – исследование нежелательных событий. Здесь реализуется определение важных РИС (с точки зрения доступности, целостности, конфиденциальности) и всех угроз, которые могут привести к нарушению безопасности (их источники и вероятности).

Модуль 3 – исследование сценариев угроз, который ориентирован на выявление и оценку сценариев, что могут вызвать описанные события, отражающие риски. С этой целью исследуются источники угроз и уязвимости.

Модуль 4 – исследование рисков. Здесь непосредственно оцениваются риски реализации сценариев угроз, исследованных в модуле 3.

Таблица 1.32. Пример критериев безопасности

Критерии безопасности	Определения	Шкала уровня	Подробное описание шкалы
Доступность	Доступность ресурсов информационной системы (РИС), своевременность РИС первой необходимости	]72 ч; ∞[	РИС не доступны более 72 часов
		]24 ч; 72 ч]	РИС доступны в течении 72 часов
		]4 ч; 24 ч]	РИС доступны в течении 24 часа
		]0 ч; 4 ч]	РИС доступны в течении 4 часов
Целостность	Точность и полнота основных РИС	Выявляемые	Изменения РИС идентифицируются
		Определенные	Изменения РИС идентифицируются и определяются (локализируются)
		Целостные	Изменения РИС не осуществляются
Конфиденциальность	Основные РИС доступны только зарегистрированным пользователям	Открытые	Публичные
		Ограниченные	Доступ только для сотрудников и партнёров
		Служебные	Доступ имеют только персонал, который участвует в разработке
		Персонализированные	Доступ только для конкретных лиц

Таблица 1.33. Пример шкалы опасности

Шкала уровня	Описание
1. Незначительная	Преодоление последствий без каких-либо трудностей
2. Средняя	Преодоление последствий несмотря на ряд трудностей
3. Высокая	Преодоление последствий с серьезными трудностями
4. Критическая	Непреодолимые последствия

Таблица 1.34. Пример вероятностной шкалы реализации сценариев угроз

Шкала уровня	Описание
1. Минимальная	Не должно произойти
2. Средняя	Может произойти
3. Высокая	Возможно или точно произойдет через день-два
4. Максимальная	Произойдет в ближайшее время

Модуль 5 – исследование мер безопасности. Пятый модуль ориентирован на определение мер безопасности и реализацию их тестирования [104].

Метод ISAMM

Метод ISAMM (Information Security Assessment & Monitoring Method, разработчик Telindus S.A. (Security, Audit and Governance Services, Бельгия) основан на требованиях стандарта ISO/IEC 27002. Он основывается на трех базовых компонентах: анализ объекта, оценка риска, отчетность.

Этот количественный метод оценивания рисков ИБ отображает их через ежегодные ожидаемые убытки в денежных единицах (Annual Loss Expectancy (ALE)). На первых этапах работы с методом определяются угрозы ИБ (см. табл. 1.35) [105].

Таблица 1.35. Пример идентифицированных угроз

ХИБ	ИУ	Описание
К	С1	Внешние злоумышленники получили или получат доступ к конфиденциальной информации
К	С2	Внутренние злоумышленники получили или получат доступ к конфиденциальной информации
К	С3	Случайное раскрытие конфиденциальных данных внутренними злоумышленниками
К	С4	Случайное раскрытие конфиденциальных данных внешними злоумышленниками
Ц	I1	Модификация или повреждение внешними злоумышленниками
Ц	I2	Модификация или повреждение внутренними злоумышленниками
Ц	I3	Случайная, ошибочная модификация
Д	А1	Отказ в обслуживании или другие нарушения, вызванные злоумышленниками (вредоносным кодом)
Д	А2	Нехватка ресурсов, ноу-хау, поддержка поставщика
Д	А3	Стихийные бедствия (землетрясения, наводнения, ураганы, молнии, пожар, экстремальные погодные условия), террористические или промышленные (ударные) воздействия
Д	А4	Отключение системы на короткий период, например, из-за погодных условий
Д	А5	Непреднамеренные отключения из-за ошибок

ХИБ – характеристика ИБ; ИУ – идентификатор угрозы;
К – конфиденциальность; Ц – целостность; Д – доступность.

При оценке риска для каждой угрозы (T) оценивается вероятность ее появления – p_T и ожидаемые последствия – I_T. Ежегодные ожидаемые убытки ALE_T для конкретной угрозы T определяются произведением вероятности возникновения и воздействия угрозы (см. табл. 1.36):

$$ALE_T = p_T \cdot I_T .$$

Также вычисляется сумма

$$ALE = \sum_T ALE_T$$

по объекту оценивания [105].

Таблица 1.36. Пример оценивания рисков

Угроза	**Вероятность** (в год)	**Воздействие** (€)	**Текущие** ALE_T (€)
C1	1	2000	2000
C2	0,2	2000	400
C3	0,5	400	200
C4	0,5	2000	1000
I1	0,2	50000	10000
I2	0,04	50000	2000
I3	0,5	400	200
A1	0,2	10000	2000
A2	0,2	400	80
A3	0,1	10000	1000
A4	2	400	800
A5	0,5	2000	1000
	Всего	129600	20680

Методология IRAM$_2$

Методология IRAM$_2$ (Information Risk Assessment Methodology$_2$, разработчик Форум информационной безопасности (Information Security Forum), США) реализуется с помощью шести этапов.

Этап 1 – обзор (связан с реализацией анализа рисков).

Этап 2 – оценка воздействия (определение и оценка различных категорий воздействий на бизнес).

Этап 3 – профиль угрозы (разрабатывается модель угроз).

Этап 4 – оценка уязвимостей (выявление возможностей среды/системы насколько хорошо она может противостоять угрозам).

Этап 5 – оценивание риска (определяется соотношение вероятности реализации угрозы и величины ее воздействия (рис. 1.10)).

Этап 6 – обработка риска (реализуется разработка планов обработки рисков) [106].

Система RiskWatch

Система RiskWatch (разработчик – компания RiskWatch, США) отображает требования стандартов ISO/IEC 27001 и ISO/IEC 27002, NIST а также COBIT IV. Процесс АОР производится в четыре фазы [107].

Фаза 1 – описание ИС организации с точки зрения ИБ (определение предмета исследования). Здесь описываются такие параметры предприятия, как тип организации, состав исследуемой системы, базовые требования в области ИБ.

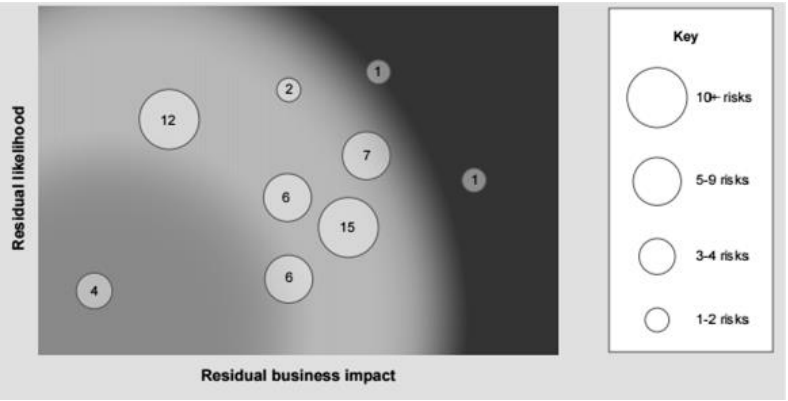


Рис. 1.10. Пример отображения риска

Фаза 2 – ввод данных. Для выявления уязвимостей инициализируется ТВ. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов (активов) (рис. 1.11), на основании чего рассчитывается эффективность внедрения средств ЗИ (СЗИ) [96].

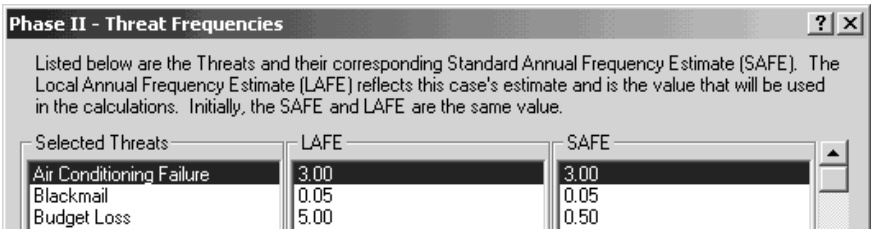


Рис. 1.11. Окно инициализации параметров

По аналогии с ПО COBRA в RiskWatch (для упрощения ввода и обработки данных) множество запросов ТВ инициируются посредством выбора данных из набора вариантов, например, конкретные числовые значения (0, 1 – «никогда», 2, 3 – «редко», 4, 5, 6 – «иногда»; 7, 8 – «обычно»; 9, 10 – «всегда») или «нет», «не знаю». Посредством запросов отражаются и оцениваются текущие правила ИБ соответственно существующим стандартам. Запросом в RiskWatch, например, может быть – «Есть ли разграничение доступа к внутренней и внешней сети, точкам доступа, отдельным компьютерам и файловым серверам?» [108].

Фаза 3 – ОР. Рассчитывается профиль рисков, и выбираются меры обеспечения ИБ. Для этого устанавливаются связи между ранее определенными ресурсами, потерями, угрозами и уязвимостями, а риск оценивается посредством ожидаемых потерь за год. Например, если стоимость сервера $v = 150\ 000\$$, а вероятность его уничтожения при пожаре в течение года p=0,01, то ожидаемые потери составят $m = 1\ 500\$$, т.е. $m = p \cdot v$, где p – вероятность возникновения угрозы, а v – стоимость ресурса. Отметим, что RiskWatch базируется на таких данных NIST, как LAFE (Local Annual Frequency Estimate) и SAFE (Standard Annual Frequency Estimate), соответственно отражающих годовую частоту реализации угроз в локализованной (например, в городе) и глобализованной (например, в Северной Америке) области. Используется также поправочный коэффициент, учитывающий частичное уничтожение ресурса. Получить оценки LAFE и SAFE, например, для Украины проблематично, поскольку нет необходимой статистики. К примеру, в США существует национальная программа по сбору данных об инцидентах (The Uniform Crime Reporting), что позволяет сформи-

ровать соответствующую статистическую информацию об инцидентах ИБ в общегосударственной базе.

Фаза 4 – генерация отчета (рис. 1.12). Формируются диаграммы и таблица детального представления соответствия и несоответствия (относительно запросов) требованиям стандарта, а также диаграмма потерь.

С учетом стоимости ресурса осуществляется оценка ожидаемых потерь (по конкретному активу) от реализации одной угрозы (*ALE*) [96, 109]

$$ALE = A \cdot EF \cdot F,$$

где:

− A – стоимость ресурса (данные, программы, аппаратура и т.д.);

− EF – коэффициент воздействия (процентная часть от стоимости актива, подвергаемой риску);

− F – частота возникновения нежелательного события.

Theft - Company Property - AFE: 2.00
The various incident classes associated with this threat are shown in the following table:

Incident Class	SLE	ALE	% of total ALE
Delays/Denials, Communications Equipment	$26,401.	$52,801.	68.0%
Delays/Denials, Data/Information	$4,400.	$8,800.	11.3%
Delays/Denials, Physical Inventory/Product	$2,750.	$5,500.	7.1%
Direct Loss, Cash	$2,200.	$4,400.	5.7%
Delays/Denials, Production Resources	$1,100.	$2,200.	2.8%
Direct Loss, Physical Inventory/Product	$1,100.	$2,200.	2.8%
Direct Loss, Data/Information	$550.	$1,100.	1.4%
Direct Loss, Production Resources	$275.	$550.	0.7%
Direct Loss, Communications Equipment	$39.	$77.	0.1%

Рис. 1.12. Фрагмент отчета в RiskWatch

Например, пусть аппаратное средство стоит A=10 000$, коэффициент воздействия на него EF=0,5, а частота F=0,2, то ожидаемые потери составят AEL=1000$. После идентификации активов и воздействий оценивается общий риск для ИС (сумма всех частных значений). Дополнительно используются показатели *ARO* – ожидаемая годовая частота происшествия и *SLE* – ожидаемый единичный ущерб (разница первоначальной и остаточной (после происшествия) стоимости актива).

Для оценивания отдельно взятой пары «угроза-ресурс» используется формула $ALE = ARO \cdot SLE$. Также применяются сценарии

«что, если:», позволяющие описать аналогичные ситуации при условии внедрения средств защиты.

Сравнивая ожидаемые потери при условии внедрения защитных мер и без них, можно оценить эффект от таких мероприятий. Для этого в RiskWatch содержатся не только базы данных LAFE и SAFE, но и базы различных СЗИ. Эффект от внедрения средств безопасности определяется параметром *ROI* – возврат инвестиций, показывающий отдачу от вложений за период времени.

Инструментарий RA2 art of risk

Инструментарий RA2 art of risk (RA Software Tool, разработчик – компании AEXIS Security Consultants и XiSEC Consultants Ltd., Великобритания) представляет собой ПО для реализации системы менеджмента информационной безопасности (СМИБ) соответственно требованиям ISO/IEC 27001:2005.

Состоит из восьми модулей:

- область СМИБ и масштабы ОР;
- идентификация активов;
- оценка активов;
- ОУ/уязвимостей;
- идентификация и ОР;
- решения по обработке риска;
- утверждение принимаемых мер;
- выполнение мер и отбор средств управления.

В процессе выполнения каждого модуля производится инициализация запросов с помощью выбора фиксированных значений в бинарно-лингвистической форме («да», «нет»). Для ОР используются восемь уровней:

1 – тривиальный;

2, 3 – минорный;

4, 5 – значительный;

6, 7 – большой;

8 – катастрофический, а матрица риска, строится на основе уровней опасности предприятия и вероятности риска в лингвистических шкалах. Значение риска формируется в виде уровней по каждой представленной категории в лингвистическом и цифровом виде, например, значению «большой уровень» соответствует число 7 [27].

Инструментарий PTA

Инструментарий PTA (Practical Threat Analysis, разработчик PTA Technologies, Израиль) основан на требованиях стандарта ISO/IEC 27001 и PCI DSS 1.1 и представляет собой программную систему для разработки модели угроз, оценивания рисков ИБ и составления планов по их снижению. Все перечисленные процессы реализуются посредством четырех шагов.

Шаг 1 – определение РИС. Здесь реализуется идентификация РИС с указанием их стоимости, связанных с ними угроз, процентное соотношение от общей стоимости всех РИС системы. Также каждому ресурсу присваивается идентификатор, например, A003 (см. рис. 1.13) [110].

Шаг 2 – выявление уязвимостей. На этом шаге анализируются и фиксируются все уязвимости (рис. 1.14) и угрозы, к которым они могут привести. Также здесь реализуется оценивание рисков как соотношение вероятности реализации угрозы и ущерба от ее реализации (рис. 1.15) [110].

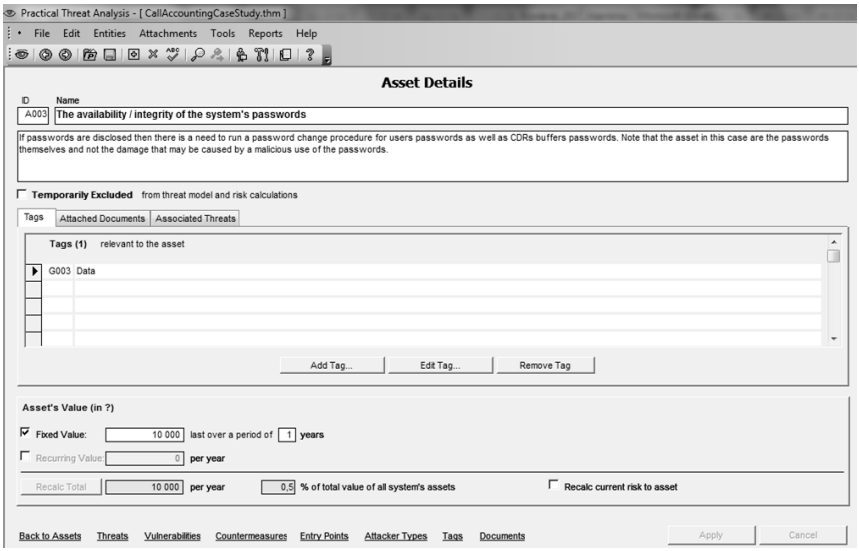


Рис. 1.13. Пример формы для идентификации РИС

Шаг 3 – определение контрмер. Этот шаг подразумевает выбор контрмер для перекрытия уязвимости и предотвращения реализации угроз (см. рис. 1.15 и 1.16).

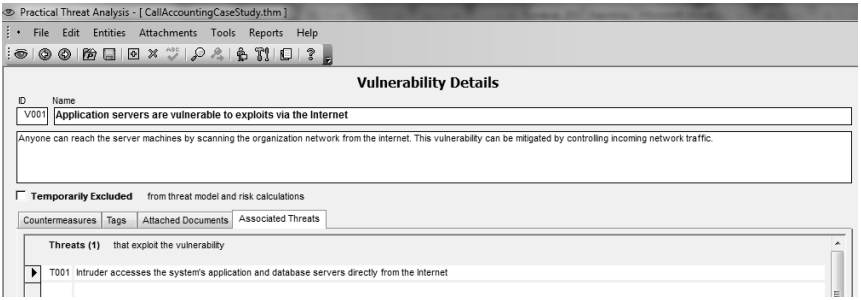


Рис. 1.14. Пример формы для фиксирования уязвимостей

Шаг 4 – разработка планов нейтрализации сценариев угроз (рис. 1.17) [110].

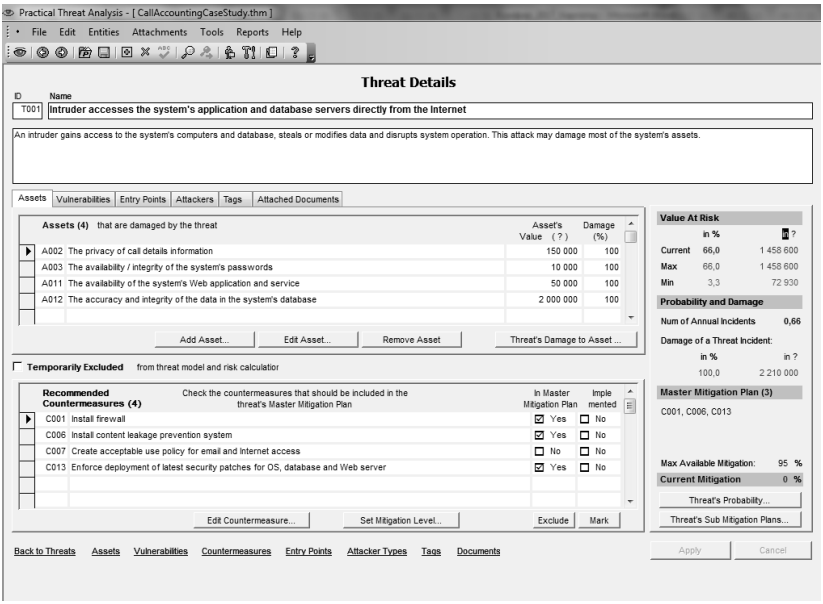


Рис. 1.15. Пример формы для фиксирования угроз и оценивания риска

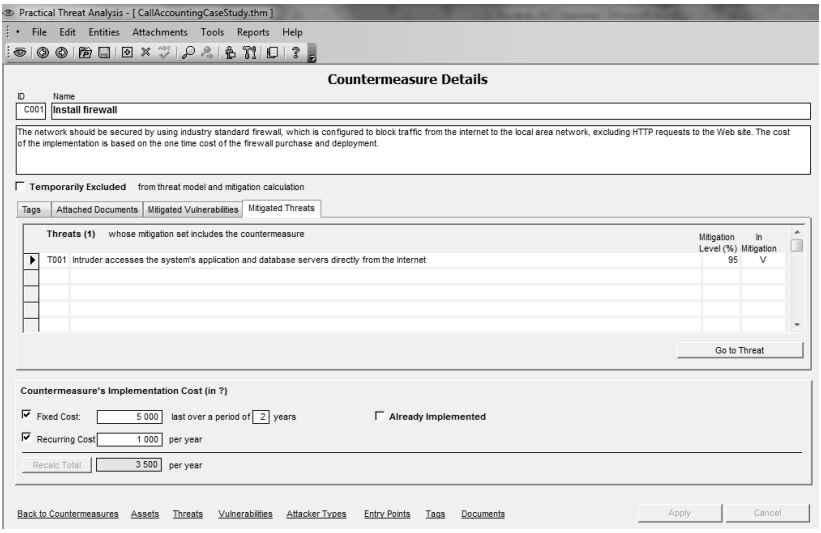


Рис. 1.16. Пример формы для фиксирования контрмер

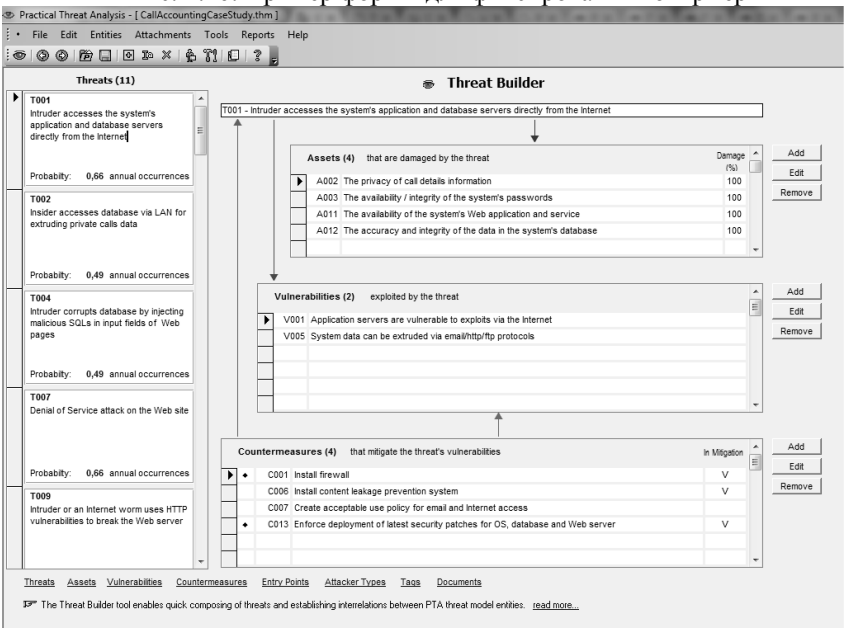


Рис. 1.17. Пример взаимосвязи РИС, уязвимости, угрозы и контрмер

Система КЭС управления ИБ «АванГард»

Система КЭС управления ИБ «АванГард» (Комплексная экспертная система «АванГард», разработчик – Лаборатория системного анализа проблем информатизации Института системного анализа РАН, Россия) включает комплекс методик:

− идентификации критически важных сегментов и объектов информационной инфраструктуры на основе АОР нарушения ИБ автоматизированных ИС (АИС);

− управления рисками нарушения ИБ больших компьютеризированных организационных систем;

− построения системы требований ИБ критически важных сегментов и объектов АИС;

− мониторингового контроля над состоянием критически важных сегментов и объектов АИС.

Основывается система на двух программных комплексах – «АванГард-Анализ» и «АванГард-Контроль» [111].

Изначально производится анализ событий риска посредством построения их моделей с помощью интерфейса главной формы (рис. 1.18), где в верхнем секторе содержится таблица со списком моделей событий рисков, по каждой из которых в заданных графах указываются экспертные оценки цены риска (в условных единицах) и вероятности (в процентах) его событий. При материальном ущербе условной единице рекомендуется присваивать ценовой эквивалент, например, 1000 руб.

При событиях риска, ущерб от которого сложно оценить в денежном выражении, используются балльные оценки, по которым ранжируются события риска по степени их опасности. В графе «Ущерб» идентифицируется расчетное значение риска по произведению его цены на вероятность.

В следующем секторе представлена таблица угроз, реализация которых может привести к событию риска. Для каждой из угроз указывается вес заданного события (рискообразующий потенциал (РП) угрозы по событию риска).

Для оценки необходимо:

− выбрать класс объекта с описанием действия, которое приводит к риску (определить его идентификатор);

− для каждого риска установить денежный эквивалент;

− рассмотреть события риска, которые могут возникнуть в результате реализации этих угроз (для определения значимости угроз, входящих в состав нормативной модели) [111].

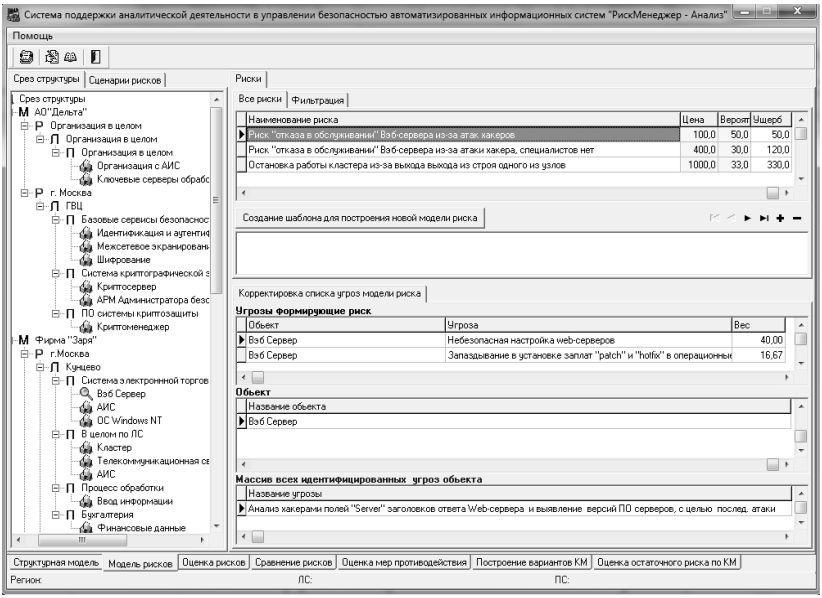


Рис. 1.18. Интерфейс построения моделей событий риска

Система Enterprise Risk Assessor

Система Enterprise Risk Assessor (Risk Advisor, разработчик – компания Methodware, Новая Зеландия) соответствует требованиям австралийского стандарта Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и ISO/IEC 17799. Представлена в трех продуктах: CobiT Advisor 3rd Edition (Audit); PRo Audit Advisor; Planning Advisor. Процесс АОР производится в три шага, что позволяет структурировать оценку, сделать её более точной.

Шаг 1: Приложение The Builder Tool – инструмент для создания структуры ОР и аудита (сбор информации). Оно позволяет построить структуру ИС, включая способность добавлять или скрывать любую часть функциональных возможностей. Основные этапы работы в этом приложении состоят из описания ИС, рисков, угроз,

потерь и анализа результатов. На этапе «Описание риска» создается матрица (рис. 1.19), позволяющая описать риски в соответствии с определенным шаблоном и задать их связи с другими элементами модели.

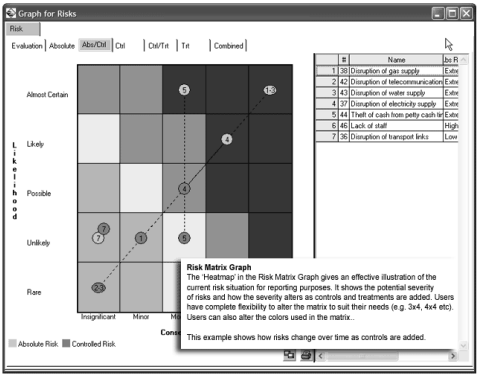


Рис. 1.19. Матрица риска

Оценка происходит на основе качественной шкалы, а риски разделяются на приемлемые и неприемлемые. Далее выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности контрмер и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах. На этапе «Описание угроз» изначально формируется список угроз, осуществляется их классификация, и описываются связи с рисками. Описание также делается на качественном уровне, что позволяет зафиксировать их взаимосвязи.

На этапе «Описание потерь» описываются события (последствия), связанные с нарушением режима ИБ. Потери оцениваются в выбранной системе критериев. Для упрощения сбора данных эксперты могут использовать ТВ, составляемый вручную. После сбора информации переходим к ОР.

Шаг 2: The Assessor – экспертная оценка (анализ собранной информации).

Шаг 3: The Consolidation Tool – инструмент консолидации (интегрирует все индивидуальные ОР). После построения модели формируется отчет (около 100 разделов) и агрегированное описание в виде графа рисков [27, 112].

В отчете (рис. 1.20) с вероятностно-лингвистической шкалой риск представлен в виде матрицы с градациями: почти наверняка, вероятно, возможно, маловероятно, редко. На рис. 1.21 представлено пример описания и ОР.

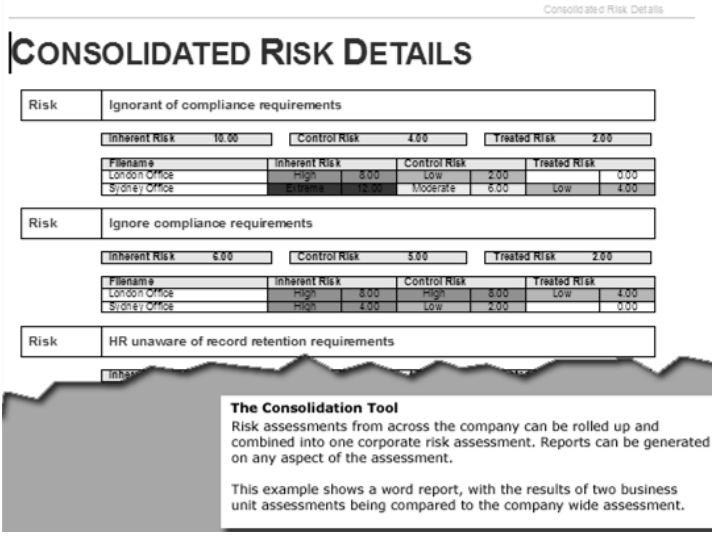


Рис. 1.20. Фрагмент отчета

Система vsRisk, Risk Assessment Tool

Система vsRisk, Risk Assessment Tool (разработчик – компания Vigilant Software Ltd., Великобритания) предназначена для ОР ИБ в соответствии с требованиями ISO/IEC 27001 и BS 7799-3.

Для упрощения процедуры АОР используются формы, для которых выбираются шкалы (устанавливаются уровни) вероятности и воздействия. Далее каждому действию определяется вероятность по выбранной шкале (рис. 1.22, а).

Система предоставляет средства для оценки всех факторов рисков, включая угрозы, уязвимости, активы и механизмы контроля и не содержит средств для количественной оценки величины риска, ограничиваясь только качественными шкалами.

Отметим, что для оценки задаются масштабы вероятности и воздействия рассматриваемых угроз. Все изменения, вносимые в базу данных продукта по ходу работы, подробным образом фикси-

руются в журнале аудита. После анализа рисков выдается оценка в виде выбранного бала для вероятности, например, 2. По результатам оценки генеруются «Декларации о применимости механизмов контроля» и «План обработки рисков» в соответствии с требованиями стандарта ISO/IEC 27001. В дальнейшем эта информация используется при выводе рекомендаций на соответствие этому стандарту. В vsRisk нет детальной ОР с описанием дальнейших рекомендуемых действий (рис. 1.22, б) [113].

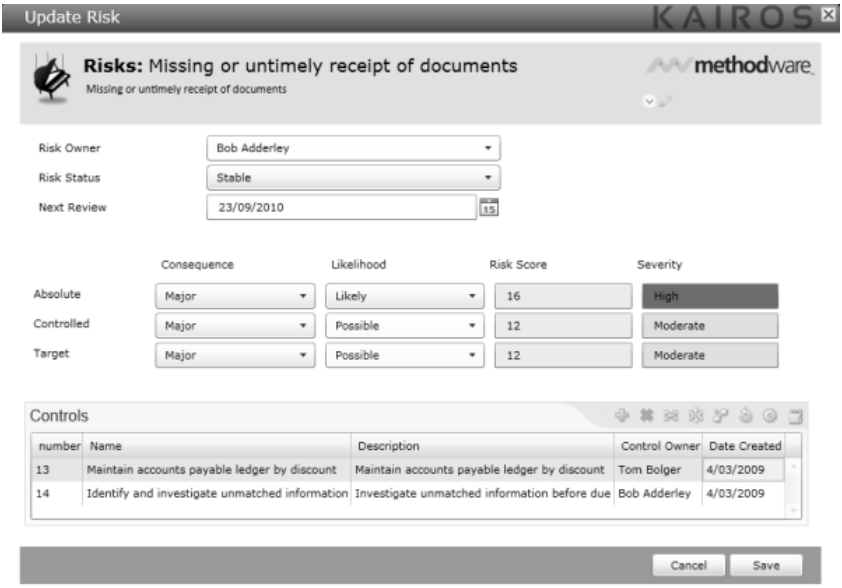
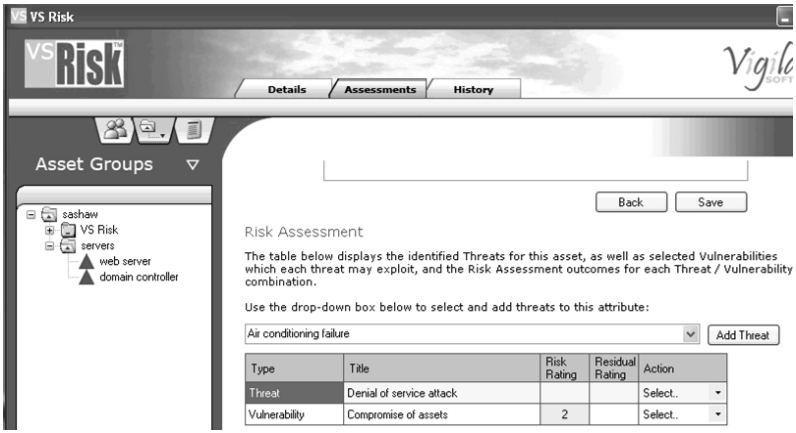


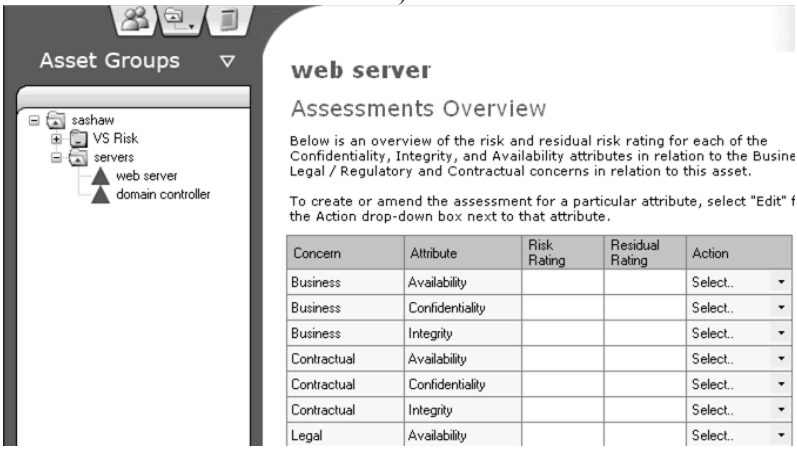
Рис. 1.21. Пример описания риска

Система OCTAVE

Система OCTAVE (разработчик – институт Carnegie Mellon Software Engineering Institute и Центр обучения, исследований и технологий (CERT), реализован в линейке продуктов: метод OCTAVE, OCTAVE-S и OCTAVE Allegro – для крупных, средних и малых организаций соответственно, США) использует трехэтапный подход для изучения организационных и технических вопросов.



а)



б)

Рис. 1.22. Пример работы системы:
а) фрагмент интерфейса ОР; б) краткий обзор оценок.

Этап 1 – «Идентификация активов и уязвимостей» состоит из четырех процессов:

− «Идентификация ресурсов управления» (собирается информация о важных активах, требованиях ИБ, угрозах и уязвимостях от представителей компании);

− «Идентификация эксплуатационных ресурсов» (собирается информация, как в предыдущем процессе, с отобранных эксплуатационных областей);

− «Идентификация ресурсов штата» (собирается информация аналогично с предыдущими процессами, от общего штата отобранных эксплуатационных областей);

− «Создание профилей угроз» (выбирается 3 ÷ 5 критических ресурсов, для которых и определяются профили угроз).

Для прохождения этого этапа в системе предлагается инициализировать ТВ (рис. 1.23, а).

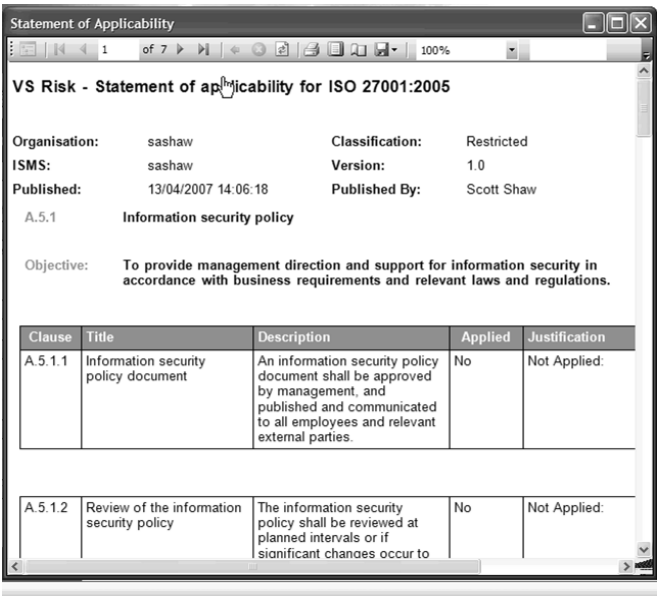
Этап 2 – «Идентификация угроз и уязвимостей инфраструктуры». Содержит два процесса:

− «Идентификация ключевых компонент» (составляется представительный набор ключевых компонент системы, которые поддерживают или обрабатывают критические информационно-связанные активы);

− «Оценка отобранных компонент» (производится оценка отобранных компонент и анализ результатов (рис. 1.23, б)).

Container Type	Questions to Consider
Technical (*see* **Worksheet 9a**)	*Internal* ❑ What information systems use or process this information asset? *Example:* • *The vendor database (information asset) is used by the accounts payable system (system).* ❑ What automated processes are reliant on this information asset? *Example:* • *Paying an invoice (process) requires information in the vendor database (information asset) and is automated in the accounts payable system (system).* ❑ On what hardware might this information asset be found? Consider: • If the information asset is used by a system, application, or process, what underlying hardware is related to the information asset? *Examples:* • *The vendor database is stored on the "DIAMOND" server.* *External*

а)



б)

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	**8**
Financial	5	Low (1)	**5**
Productivity	3	Low (1)	**3**
Safety and Health	1	Low (1)	**1**
Fines/Legal	2	High (3)	**6**
		Total Score	**23**

в)

Рис. 1.23. Пример работы системы:
а) фрагмент запросов для этапа 1; б) отчет соответствия;
в) результат оценки общего риска

Угрозы разделяют на следующие категории:

- с участием человека и использованием технических средств;
- с участием человека и использованием физического доступа;
- технические проблемы;
- другие проблемы.

В процессе прохождения этапа 2, риск определяется как функция $R(T,I)$, где T – угроза (threat)/условие (condition), а I – воздействие (impact)/следствие (consequence). Также детально описывается ущерб, который будет нанесен компании в случае наступления ситуации риска.

Этап 3 – «Развитие стратегии и планов безопасности» (идентифицируются риски к критическим активам организации и принимаются решения по их обработке). Состоит из двух процессов:

- «АОР» (определяется уровень воздействия (высокое, среднее, низкое) угроз критическим активам);
- «Развитие стратегии защиты» (команда развивает стратегию защиты всей организации, сосредотачиваясь на улучшении методов обеспечения ее ИБ [114]).

Пример процесса оценки (при этом используется шкала – средний, низкий, высокий), относительно заданной сферы действия риска рассмотрен в табл. 1.37.

В дальнейшем при общей оценке для каждой сферы присваивается коэффициент уровня риска:

- высокий – 3,
- средний – 2,
- низкий – 1.

Полученные балы по каждой угрозе в процессе АОР суммируются (рис. 1.23, в).

Таблица 1.37. Пример процесса ОР

Сфера действия риска	Уровень риска
репутация / доверие клиентов	средний
финансы	низкий
производительность	низкий
безопасность и здоровье	низкий
штрафы	высокий

Инструментарий Callio Secura 17799

Инструментарий Callio Secura 17799 (разработчик – компания Callio Technologies, Канада) является Web-приложением, включающим все необходимое для менеджера при разработке, внедрении,

управлении и сертификации СМИБ, согласно ISO/IEC 17799/BS7799 [115].

Система содержит четыре секции:

− «Методология» – помощник, объясняющий шаги правильного осуществления внедрения ISO/IEC 17799 и продвижения к сертификации BS 7799-2;

− «Администрирование» – инструментарий для правильного определения структуры управления СМИБ;

− «Инструменты» – набор инструментов для реализации правильного выполнения требований ISO/IEC 17799;

− «Управление ИБ» – модули, позволяющие эффективно управлять рисками организации и подготовиться к аудиту СМИБ. Для ОР ИБ необходимо инициализировать ТВ составленный согласно требованиям стандарта [116].

Процесс АОР проходит в два этапа, на первом – производится идентификация активов, угроз, уязвимостей и требований ИБ, оценивается величина уязвимостей, вероятность угроз и ценность активов, определяемая ущербом в результате нарушения конфиденциальности, целостности, доступности (рис. 1.24). С использованием этих данных вычисляется значение риска [116].

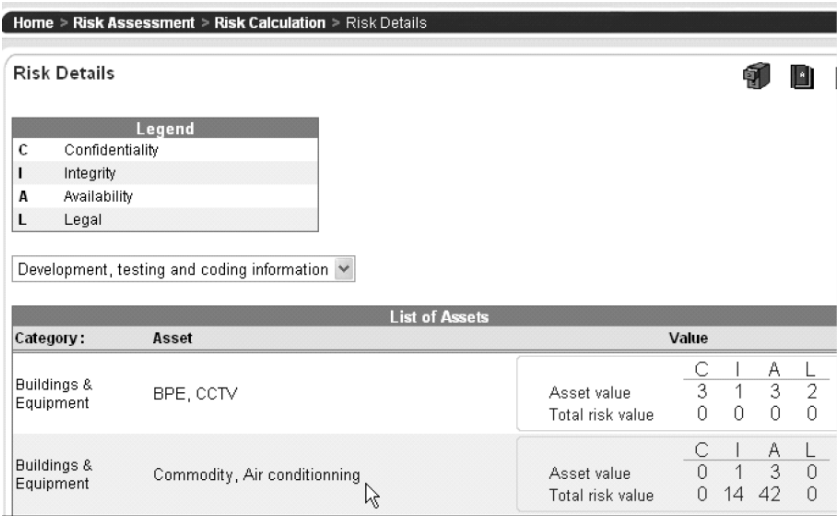


Рис. 1.24. Пример ОР

На втором этапе принимается решение относительно способов обработки рисков и приемлемого уровня остаточных рисков, создается план обработки рисков, производится внедрение механизмов контроля и разработки политики ИБ и других организационно-распорядительных документов.

В ходе описания необходимо задать данные относительно критериев «высокий» – (3), «средний» – (2), «низкий» – (1) [117]. Базируясь на информации о ценности активов и вероятности угроз, автоматически вычисляются значения рисков, и производится их упорядочивание по приоритетам (риск относительно конфиденциальности, целостности, доступности и законности).

Система Гриф 2006

Система Гриф 2006 (разработчик – компания Digital Security, Росия) направлен на обеспечение самостоятельной работы ИТ-менеджера (без привлечения сторонних экспертов) по оценке УР в ИС и эффективности существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство в необходимости инвестиций в сферу ИБ. Процесс АОР в системе Гриф 2006 состоит из 3 этапов.

Этап 1 – составление модели анализа информационных потоков (описание активов компании и всех бизнес-процессов).

Этап 2 – создание модели анализа угроз и уязвимостей. Для оценки используется разработанная Digital Security классификация угроз, в которой описаны все действия, рассматриваемые во время оценки способные привести к нарушению базовых характеристик ИБ, то есть к событиям нарушения ИБ.

Этап 3 – указание ущерба для каждой группы ценных ресурсов, по всем видам угроз. На этом этапе необходимо инициализировать ТВ по политике ИБ, реализованной в системе, что позволит оценить реальный уровень ее защищенности и детализировать ОР. Анализ рисков ИБ осуществляется с помощью построения модели ИС организации [96].

Риск оценивается отдельно по каждой связке «группа пользователей – информация», т.е. модель рассматривает взаимосвязь «субъект – объект», с учетом всех их характеристик.

Рассчитываются вероятность реализации угрозы, ее уровень по уязвимости на основе критичности и вероятности реализации через данную уязвимость и возможный ущерб. В системе используется шкала от 0 до 100%.

Система @RISK

Система @RISK (разработчик – компания Palisade, США) предназначена для АОР с помощью метода Монте-Карло [118], реализуемого на основе Microsoft Excel. Система позволяет проследить возможность принятия и избежания рисков, а также принимать наилучшие решения в условиях неопределенности. Для ОР также используется метод Value at Risk (VAR) [100].

На начальном этапе работы производится создание модели оценки (анализ риска), посредством заполнения таблицы (см. пример табл. 1.38). Далее происходит расчет расходов если произойдёт ситуация нарушения ИБ.

Таблица 1.38. Пример таблицы эксплуатационных рисков

Эксплуатационные риски	Вероятность (годовая) %	Воздействие ($)	Среднее воздействие ($)
Отказ IT системы	0,1	1000	5
Проблема с производственным процессом	0,05	50	3
Тяжелое заболевание члена правления	0,05	100	5
Служащий выигрывает судебный процесс	0,08	250	20
Появления нового конкурента	0,25	400	100
Отказ выпуска нового товара	0,15	300	45
Укрепление ставки $	0,35	100	35
Пожар в главном офисе	0,02	250	5
Мошенничество	0,005	500	3
Потеря конфиденциальных данных	0,01	300	3
Банкротство главного клиента должника	0,02	150	3
Общие количество		**3400**	**227**

Система RiskPAC

Система RiskPAC (разработчик – компания CSCI, Нидерланды) предназначена для обнаружения и оказании помощи при устранении уязвимостей в ИС. Конструктор анкет, позволяет автоматизировать любую ручную методику ОР, для анализа которого необходимо инициализировать (с помощью фиксированных вариантов) запросы в ТВ, представленных в виде реляционных баз данных (БД). Во время ОР для подсчета вероятности угроз используется шкала: маловероятно, вероятно и весьма вероятно. Также подсчитывается воздействие по шкале: минимальное, значительное, серьёзное и катастрофическое. Дополнительно в системе содержится калькулятор ожидаемых среднегодовых потерь [112, 119].

Система Microsoft Security Assessment Tool

Система Microsoft Security Assessment Tool (MSAT, разработчик – компания Microsoft, США) базируется на материалах «Руководства по управлению рисками» [33]) выполняет следующие функции:

1) ОР;
2) поддержка принятия решений;
3) реализация контроля;
4) оценка эффективности программы.

Приложение ориентировано на организации с числом сотрудников менее 1000 человек, для содействия лучшему пониманию потенциальных проблем в сфере ИБ. В ходе работы пользователь, выполняющий роль аналитика ответственного за вопросы ИБ, работает с двумя группами запросов.

Первая из них посвящена оцениванию риска для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса. Запросы этой группы разбиты на 6 этапов:

Этап 1 – «Параметры компании» (название, число компьютеров, серверов и т.д.);

Этап 2 – «Безопасность инфраструктуры»;

Этап 3 – «Безопасность приложений»;

Этап 4 – «Безопасность операций»;

Этап 5 – «Безопасность персонала»;

Этап 6 – «Среда».

После реализации этапов этой группы осуществляется обработка (посредством подключения к Интернет) полученной информации и переход к второй группе запросов, которые организованы в соответствии с концепцией многоуровневой (эшелонированной) ЗИ. Во многом ТВ соответствует разделам стандартов ISO/IEC 17799 и ISO/IEC 27001.

После инициализации запросов клиентская часть программной системы вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес представляет «Полный отчет», содержащий предлагаемый список приоритетных действий. На этапе анализа риска производится идентификация активов, предлагается их качественная классификация (высокое, среднее и низкое влияние на бизнес), а также определяется перечень угроз и уязвимостей. На этапе ОР определяется потенциальный ущерб по трехуровневой шкале (высокая, средняя и низкая подверженность воздействию).

При оценке частоты возникновения угроз используются градации:

− высокая (вероятно возникновение одного или нескольких событий в пределах года);

− средняя (влияние может возникнуть в пределах двух-трех лет);

− низкая (возникновение влияния в пределах трех лет маловероятно).

Методика TRA

Методика TRA [48, 120] (Threat and Risk Assessment, разработчик – компания Government (Communications Security Establishment), Канада) разработана на основе трех руководств для IT-систем по:

− сертификации и аккредитации (MG-01);

− управлению риском безопасности (MG-02);

− ОР и выбору гарантий (MG-03 [120]).

Для ОР, аналитик должен рассмотреть описание IT-системы, идентифицировать существенные сценарии угроз, оценить воздействие и их ВВ (рис. 1.25).

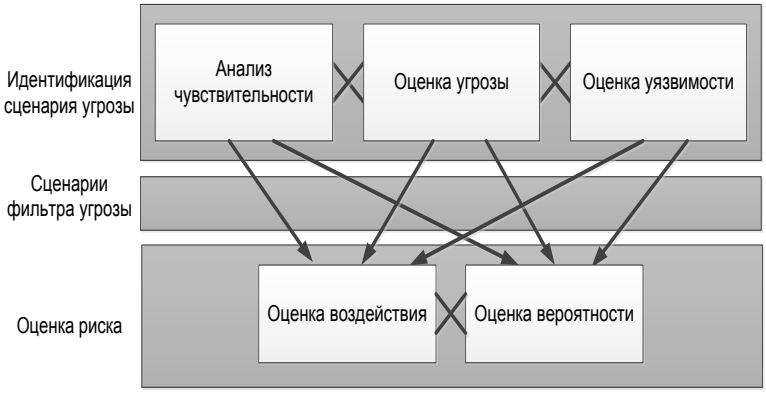


Рис. 1.25. Процесс ОР

В процессе ОР для каждого сценария угрозы рассчитываются ее воздействие и вероятность. Такой подход отображает средние ожидаемые потери за определенный период времени [48]. По сути, риск (*R*) описывается как функциональная связь между стоимостью активов (A_{Val}), угрозой (*T*) и уязвимостью (V): $R = f(A_{Val}, T, V)$.

Процесс ОУ (например, «Хакерская атака») для такой подгруппы активов, как корпоративные данные (КД) осуществляется на основе табл. 1.39 [48], где уровень нарушения таких характеристик ИБ, как К, Ц и Д отображается трехуровневой КЧ шкалой («В», «С», «Н»).

Таблица 1.39. Пример ОУ

Класс угрозы	Действие угрозы	Категория агента угрозы (АУ)	АУ	Событие угрозы	Уровень нарушения			Подгруппа активов
					К	Ц	Д	
Предна-меренная	Шпионаж	Хакеры	-	НСД	В	-	-	КД
	Саботаж	Хакеры	-	НСМ	-	-	В	КД
	Саботаж	Хакеры	-	DoS	-	Н	-	КД

Методика FRAP

Методика FRAP [121] (Facilitated Risk Analysis Process, разработчик – компания Peltier and Associates, США) ориентирована на

обеспечение ИБ ИС, рассматриваемое в рамках процесса управления рисками, состоящего из пяти этапов.

Этап 1 – Определение защищаемых активов (производится на основе ТВ, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей).

Этап 2 – Идентификация угроз. При составлении списка угроз могут использоваться разные подходы, например:

− выбор актуальных для данной ИС угроз из заранее подготовленных экспертами перечней (checklists);

− анализируется статистика инцидентов ИБ связанных с данной ИС;

− оценивается их среднегодовая частота (по ряду угроз, например, возникновение пожара, данные можно получить у соответствующих государственных организаций);

− специалисты компании решают задачу посредством «мозгового штурма» и др.

Этап 3 – ОР. Каждой угрозе из составленного списка сопоставляют ее ВВ, далее оценивают ущерб, который может быть нанесен данной угрозой и по полученным значениям, оценивается ее уровень. При проведении анализа риска, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты.

Таким образом оценивается УР для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств ЗИ. Оценка производится по ВВ угрозы и ущерба от её реализации в течение года с использованием следующих шкал. Для вероятности (Probability):

− высокая (High Probability) – вероятно;

− средняя (Medium Probability) – возможно;

− низкая (Low Probability) – маловероятно.

Для ущерба (Impact – мера величины потерь или вреда, наносимого активу):

− «В» (High Impact) – остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли;

− «С» (Medium Impact) – кратковременное прерывание работы критических процессов или систем, которое приводит к

ограниченным финансовым потерям в одном бизнес-подразделении;

− «H» (Low Impact) – перерыв в работе, не вызывающий ощутимых финансовых потерь.

Оценка осуществляется в соответствие с правилом, задаваемым матрицей рисков (рис. 1.26) и может интерпретироваться следующим образом:

− уровень *A* – связанные с риском меры (например, внедрение средств ЗИ) должны быть выполнены немедленно и в обязательном порядке;

− уровень *B* – связанные с риском меры должны быть предприняты;

− уровень *C* – требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо);

− уровень *D* – никаких мер в данный момент предпринимать не надо [121].

Этап 4 – Определение контрмер. После идентификации угроз и оценки риска определяются контрмеры, позволяющие устранить риск или свести его до приемлемого уровня.

Этап 5 – Документирование. После АОР результаты подробно документируются в стандартизованном формате. Полученный отчет может быть использован при определении политик, процедур, бюджета ИБ и т.д.

PROBABILITY **IMPACT**

	High	Medium	Low
High	*A*	*B*	*C*
Medium	*B*	*B*	*C*
Low	*B*	*C*	*D*

A – Corrective action must be implemented
B – Corrective action should be implemented
C – Requires monitor
D – No action required at this time

Рис. 1.26. Матрица рисков FRAP

Методика Risk Matrix

Методика Risk Matrix [122] (разработчик компания Mitre Corporation, США) ориентирована на АОР и впоследствии была реализована приложением для Microsoft Excel. Основной процесс включает: планирование оценки степени риска; идентификацию задач или требований; определения; ранжирование; составление рейтинга рисков; управление планами действий; непрерывную оценку рисков.

Оценки риска заключается в планировании деятельности. Изначально производится идентификация риска с помощью применения экспертами «Мозгового штурма».

Далее присваиваются различные атрибуты каждому риску, такие как, например, период времени (даты начала и окончания возможной реализации) и ВВ.

С помощью сценария «Если риск…, то последствия…» составляется матрица риска.

Для определения воздействия используется шкала:

- C (критическое);
- S (серьезное);
- M_o (средние);
- M_i (низкое);
- N (незначительное).

A для вероятности – (P):

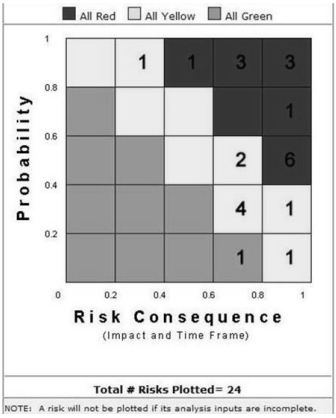
- 0-10% (очень низкая);
- 11-40% (низкая);
- 41-60% (средняя);
- 61-90% (выше среднего);
- 91-100% (высокая).

На этапе ранжирования используется метод Borda и далее составляется рейтинг риска с определением его степени – «Н», «С» или «В» табл. 1.40 [122].

Для определения наиболее приоритетных рисков используется диаграмма частот (рис. 1.27). Пример матрицы риска представлен на рис. 1.28 [122].

Таблица 1.40. Шкала риска

ПВР (%)	Категории воздействия				
	N	**M_i**	**M_o**	**S**	**C**
0-10	H	H	H	C	C
11-40	H	H	C	C	B
41-60	H	C	C	C	B
61-90	C	C	C	C	B
91-100	C	B	B	B	B



All 5x5 Cells: Red

Risk ID	Risk Name	Consequence	Probability	Mitigatio
INF.003	Platform System Integration	0.91	1.00	Yellow
MGT.001	Organizational Interfaces	0.89	0.90	White
OPS.003	Ground Sampling Collection and Analysis	0.84	1.00	Green
SE.016	Technolgy Readiness for Science Payload CIs	0.87	0.70	Red
SE.015	Cannot handle real-time transmission rate	0.91	0.60	Red
PROG.001	Stakeholder and Mission Partner Complexity	0.73	0.90	Red
SE.017	Balloon weight	0.89	0.50	White
OPS.006	Balloon inflation	0.82	0.60	Yellow
MGT.002	WBS	0.81	0.60	White
OPS.009	Accurately controlling vehicle altitude in the Venusian environment	0.84	0.50	White
SE.005	Component single point of failure	0.81	0.50	Green
APPS.001	SW Testing Enviroment	0.67	1.00	Yellow

Рис. 1.27. Диаграмма частот

Методика Mehari

Методика Mehari (называют методологией) [123] (разработчик Clusif, Франция) заменила систему Clarion и предоставляет собой структурированный подход к оценке рисков. Она дает возможность КЧ и КЛ оценить факторы риска и УР. При этом Mehari интегрирует инструменты (например, критерии оценки, формулы и т.д.) и базы знаний (в частности, меры для диагностики ИБ), являющиеся важным дополнением к минимальным методам предложенных в ISO/IEC 27005:2008.

Для того, чтобы ответить на вопрос «Какие риски являются высокими для организации и приемлемые они или нет?» применяется структурированный подход, чтобы выявить все возможные события риска, анализировать индивидуально наиболее важные из них,

а затем определить действия по снижению риска до приемлемого уровня.

	A	B	F	G	H	J	K	O	P	U
1	Risk No.	Related Risk	RISK	Timeframe Start	Timeframe End	I	Po (%)	Borda Rank	R	Manage/Mitigate
2	1	4	IF contract is not awarded before 30 Sep, THEN program loses $8M in expiring funds.	30 Jan 1999	30 Sep 1999	C	60%	0	H	Use existing Task Order contract to assure award before 30 Sep.
3	2	N/A	IF unmodified commercial laptops are used, THEN operational availability cannot be met in intended environment.	28 Feb 1999	28 Feb 2000	S	100%	0	H	Limit buy for first release and plan technology insertion for improved environmental performance for second release.
4	3	4	IF DII COE V1.5 is more than 1 mo. late, THEN first release will slip day for day.	30 Jan 1999	30 Oct 1999	S	90%	3	M	Use DII COE V1.4 for first release and modify requirements.
5	4	1,3	IF first release is not demonstrated in EFX, THEN program will be assigned to Navy.	15 Feb 1999	15 Apr 2000	C	60%	0	H	Integrate only those capabilities available at contract award for first release.
6	5	1	IF all KPPs must be satisfied by second release, THEN program funding is insufficient.	30 Jan 1999	30 Jul 2001	S	40%	4	M	Use CAIV to prioritize release content subject to budget and plan for third and fourth release.

RiskEntries / ChartI / ChartPo

Рис. 1.28. Пример матрицы риска

Для оценки предлагаются два основные варианта – использовать базы знаний (которые интегрируются в Microsoft Excel, Open Office) или ПС (например, Risicare которое обеспечивает более богатый пользовательский интерфейс, а также позволяет моделировать, визуализировать и оптимизировать полученные результаты).

Для оценки используется структурированная модель риска, которая учитывает «факторы снижения риска» [124]. Процесс АОР реализуется в 9 этапов:

1. Идентификация риска. Предлагаются два подхода – прямой (предусматривает идентификацию неисправностей или событий, которые могут привести к нарушению ИБ, в результате будут описаны возможные типы неисправностей) и системный (заключается в использовании обширных баз знаний для ведения автоматизированной оценки).

2. Оценка воздействия. Здесь используется КЧ шкала где:

− 1 – очень низкая экспозиция (независимо от любых мер ИБ, вероятность того, что такой сценарий будет происходить – очень низкая);

− 2 – низкое воздействие (вероятность того, что такой сценарий произойдет в краткосрочный или среднесрочный период – низкая);

− 3 – средняя экспозиция (если ничего не предпринимать, то такой сценарий должен произойти в более или менее короткий срок);

− 4 – высокий уровень воздействия (если ничего не будет сделано, то такой сценарий неизбежен в очень короткий срок).

3. Оценка сдерживающих факторов. Проводится аудит сдерживающих и профилактических факторов, которые могут предотвратить возникновения риска.

4. Оценка защитных, паллиативных и рекуперативных факторов.

5. Оценка потенциальности. Оцениваются потенциальные риски (которые должны произойти) на основании пятибалльной шкалы:

− 0 – отсутствует;

− 1 – очень маловероятно;

− 2 – маловероятно;

− 3 – скорее всего;

− 4 – очень вероятно.

6. Оценка влияния. Производятся оценки последствий наступления риска независимо от любых мер ИБ.

7. Оценка воздействия после принятия мер по снижению риска и показателей сокращений воздействия.

8. Глобальная ОР. Определяются глобальные риски для организации.

9. Принятия решения о приемлемости или неприемлемости риска [123].

Методика MAGERIT

Методика MAGERIT [125] (Methodology for Information Systems Risk Analysis and Management, разработчик Ministerio De Administraciones Públicas, Испания) предназначена для реализации процесса АОР, который проводится в 3 этапа:

Этап 0 – Планирование.

Этап 1 – Анализ риска. Состоит из 5 шагов:

1. Идентификация и оценка активов, являющихся элементами ИС (или тесно связанных с ней) ценными для организации. Активы

предлагается разделять на 5 групп (окружающая среда, ИС, информация, функции организации, другие активы) для определения зависимости между ними. После ранжирования активов производится их оценка относительно стоимости. Далее определяются требования к К, Ц и Д и подлинности актива;

2. Анализ и ОУ ИБ. С помощью категории угроз, которые приведены в данной методике, производится их идентификация, реализуется оценка частоты (используется шкала: 100 – очень часто (ежедневно); 10 – часто (ежемесячно); 1 – обычно (ежегодно); 1/10 – редко (раз в несколько лет)) и ущерба;

3. Определение превентивных мер для предотвращения угрозы;

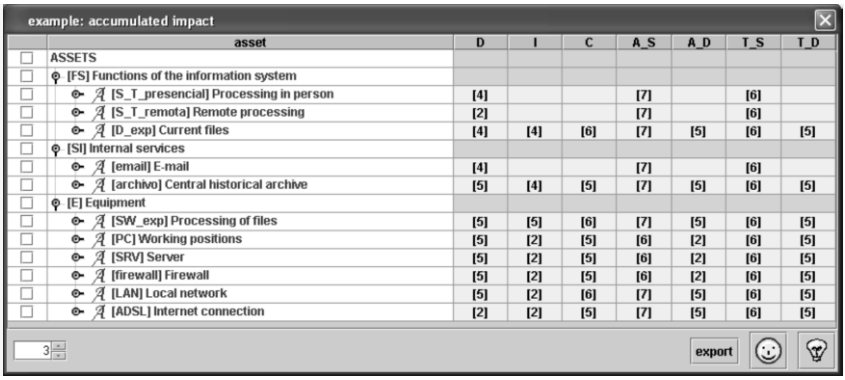
4. Оценка воздействия. Измерение повреждения активов, связанного с угрозой;

5. Определение риска. Риск отражается вероятностью повреждения ИС и увеличивается с ростом воздействия и частоты (табл. 1.41 [125]).

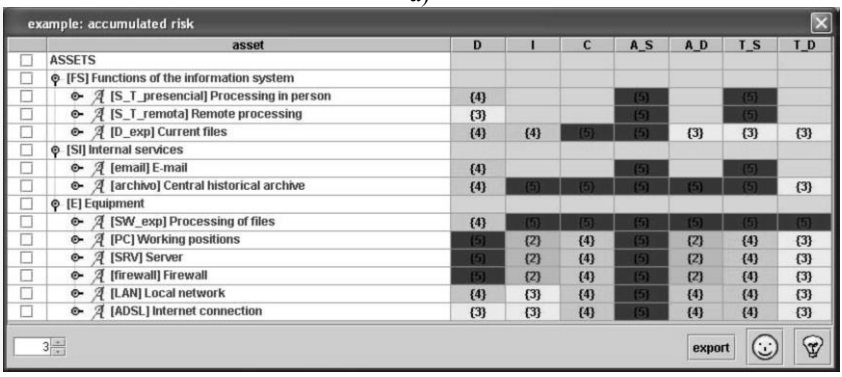
Таблица 1.41. Пример потенциальных угроз файлам данных

		Измерение ИБ (%)						
актив/угроза	**F**	**D**	**I**	**C**	**AS**	**AD**	**TS**	**TD**
[D_exp] Текущие файлы		**50**	**50**	**100**	**100**	**100**	**100**	**100**
[E.1] Ошибки пользователей	10	10	10					
[E.2] Ошибки администратора	1	20	20	10	10	10	20	20
[E.3] Ошибки мониторинга	1						50	50
[E.4] Ошибки конфигурации	0,5	50	10	10	50	50	50	50
[A.4] Изменения конфигурации	0,1	50	10	50	100	100	100	100
[A.11] Несанкционированный доступ	100		10	50	50			

Этап 2 – Управление рисками. Выбираются и реализуются защитные меры (технические, физические [126], защиты рабочей среды для людей и оборудования, организационные меры, кадровая политика), а также осуществляется интерпретация значения для воздействия и остаточных рисков, проводится анализ прибыли и убытков [125]. Примеры оценок показаны в ПО «Techniques Guide» на рис. 1.29 а-б, где D, I и C – соответственно К, Ц и Д данных, AS и AD – соответственно подлинность пользовательских услуг и происхождения данных TS и TD – соответственно подотчетность использования услуг и доступа к данным [75, 125].



а)



б)

Рис. 1.29. Пример оценки: а) воздействия; б) риска

Методика Information Security RA

Методика Information Security RA [127] (Risk Assessment, разработчик Centers for Medicare & Medicaid Services (CMS), США) предоставляет возможность реализации АОР в сфере ИБ.

Методика состоит из 3 фаз:

Фаза 1. Документирование системы. Фаза реализуется в нескольких процессах – идентификация системной документации и активов, а также определение текущего уровня ИБ (с использованием шкалы: «В», «С» и «Н» табл. 1.42 [127]);

Фаза 2. Определение риска. Расчет УР для каждой пары угрозы и уязвимости, на основе вероятности того, что угроза с использованием уязвимости будет осуществлена. Также определяется сте-

пень воздействия, которую угроза окажет на ИС (ее данные и бизнес-функции) с точки зрения потери К, Ц и Д. Фаза 2 состоит из 6 шагов:

1. Выявление угрозы;
2. Определение уязвимости;
3. Выявление существующих элементов управления для снижения риска реализации данной угрозы (с использования уязвимости).
4. Определение ее ВВ с учетом существующих элементов управления, для чего используется семиуровневая шкала:
   - НЗ – незначительная (маловероятно);
   - ОН – очень низкая (вероятно два/три раза в пять лет);
   - Н – низкая (произойдет один раз в год или меньше);
   - С – средняя (может произойти один раз в шесть месяцев или менее);
   - В – высокая (произойдет один раз в месяц или меньше);
   - ОВ – очень высокая вероятность (несколько раз в месяц);
   - ЭВ – экстремально вероятно (несколько раз в день).
5. Оценивание степени воздействия на систему осуществляется по шестиуровневой шкале:
   - НЗ – незначительное;
   - МЛ – малое;
   - ЗН – значительное;
   - ПВ – повреждающее;
   - СЕ – серьезное;
   - КР – критическое.
6. Определение УР для данной пары угроза – уязвимость существующих элементов управления. УР определяются согласно табл. 1.43 [86, 87, 92, 127-129].

Таблица 1.43. Уровни риска

ВВ	**Воздействие**					
	НЗ	**МЛ**	**ЗН**	**ПВ**	**СЕ**	**КР**
НЗ	Н	Н	Н	Н	Н	Н
ОН	Н	Н	Н	Н	С	С
НК	Н	Н	С	С	В	В
СР	Н	Н	С	В	В	В
ВС	Н	С	В	В	В	В
ОВ	Н	С	В	В	В	В
ЭВ	Н	С	В	В	В	В

1.7. Современные базы данных уязвимостей информационной безопасности

При построении различных систем ЗИ (например, СМИБ [1] или КСЗИ [2]) возникает необходимость осуществлять оценивание состояния ИБ, с учетом известных уязвимостей РИС. Поэтому перед специалистами, занимающимися исследованием состояния безопасности ИС, возникает вопрос о эффективности использования соответствующих БД уязвимостей, удовлетворяющих определенным критериям [2, 130-134], таким, например, как наличие идентификаторов CVE, оценок CVSS, CWE категорий, CVSS-калькулятора, риск-калькулятора и д.р. Использование указанных критериев позволит осуществить рациональный выбор таких БД. В связи с этим актуальной является задача исследования соответствующих БД для определения набора критериев, согласно которых можно эффективно использовать такие базы.

На сегодняшний день существует широкое множество общедоступных БД уязвимостей РИС, которые подвергались анализу в различных источниках. Так, в работе [132] проводилось исследование открытых БД уязвимостей, где авторами были определены основные поля записей уязвимостей, достоинство и недостатки рассматриваемых баз, но не определенны обобщенные критерии, по которым можно осуществлять такой анализ. Также в работах [133-135] рассмотрены БД с точки зрения наличия ссылок на другие базы, возможности получения информации в формате XML, а также формате представления уязвимостей в БД. Следует отметить, что в [133, 135] не определены четкие критерии, по которым можно осуществить соответствующий анализ. Авторами работы [134], при обосновании выбора БД, за основу были приняты следующие критерии: полнота (емкость, количество уязвимостей); доступность данных (бесплатная база); удобство получения данных (интерфейсы); поддержка оценки уязвимостей по системе CVSS, но больше делался акцент на уязвимости, влияющие на доступность. Также следует отметить, что в работах [130-135] не были четко выделены критерии, по которым можно сравнить БД уязвимостей и осуществить их выбор для построения различных систем оценивания в области ИБ, например, таких как системы АОР.

В связи с этим, осуществим исследование широкого спектра существующих БД уязвимостей для определения критериев, по которым можно осуществить сравнительный анализ таких баз и использовать их при анализе и оценивании рисков ИБ.

Для проведения такого исследования, воспользуемся наиболее известными и общедоступными БД уязвимостей:

− национальная БД уязвимостей – National Vulnerability Database (NVD), (США) [136];

− банк данных угроз безопасности информации (Российская Федерация) [137];

− открытая БД уязвимостей – Open Sourced Vulnerability Database (OSVDB), (США) [138];

− БД уязвимостей IBM X-Force, (США) [139];

− БД записей уязвимостей US-CERT – Vulnerability Notes Database US-CERT (VND), (США) [140];

− БД уязвимостей SecurityFocus, (США) [141].

Рассмотрим каждую из них.

National Vulnerability Database

База National Vulnerability Database разработана National Institute of Standards and Technology (NIST) Computer Security Division, Information Technology Laboratory при поддержке Department of Homeland Security's National Cyber Security Division. Она является государственным хранилищем данных США, которое основано на стандартах управления уязвимостями. Такие данные позволяют автоматизировать процессы управления уязвимостями, измерять состояние ИБ и определять его соответствие. База NVD включает в себя БД контрольных списков безопасности, недостатков РИС, неправильных конфигураций, РИС и показателей воздействия.

Рассматриваемая БД представляет собой репозитарий основных стандартов управления данными уязвимостей, разработанный на основе протокола автоматизации контента безопасности – Security Content Automation Protocol (SCAP) [136].

Существуют следующие компоненты SCAP:

− БД уязвимостей безопасности – Common Vulnerabilities and Exposures (CVE);

− БД уязвимых конфигураций РИС – Common Configuration Enumeration (CCE);

− стандартная номенклатура и база имен РИС – Common Platform Enumeration (CPE);

− БД слабых мест – Common Weakness Enumeration (CWE);

− стандарт оценки влияния уязвимостей – Common Vulnerability Scoring System (CVSS);

− стандарт XML-спецификации контрольных листов – Extensible Configuration Checklist Description Format (XCCDF);

− стандарт XML-спецификации контроля состояний процессов – Open Vulnerability and Assessment Language (OVAL) [136].

Кроме этого применяется следующий набор других протоколов.

Threat Analysis Automation Protocol (TAAP) – протокол документирования и совместного использования структурной информации об угрозах. Он содержит следующие компоненты:

− БД атрибутов вредоносного ПО – Malware Attribute Enumeration & Characterization (MAEC);

− БД шаблонов атак – Common Attack Pattern Enumeration & Classification (CAPEC);

− CPE;

− CWE;

− OVAL;

− CCE;

− CVE.

Event Management Automation Protocol (EMAP) – протокол для отчетов о событиях безопасности. Он имеет следующие составляющие:

− БД записей событий – Common Event Expression (CEE);

− MAEC;

− CAPEC.

Incident Tracking and Assessment Protocol (ITAP) – протокол для отслеживания, документирования, управления и совместного использования информации об инцидентах. Он содержит следующие компоненты:

− OVAL;

− CPE;

− CCE;

- CVE;
- CVSS;
- MAEC;
- CAPEC;
- CWE;
- CEE;
- формат обмена описанием инцидента – Incident Object Description Exchange Format (IODEF);
- национальная модель обмена информацией – National Information Exchange Model (NIEM);
- формат обмена информацией по кибербезопасности – Cybersecurity Information Exchange Format (CYBEX) [136].

Рассмотренные протоколы, стандарты и базы данных NVD на практике, например, можно использовать в следующих целях:

- CPE – определение ИС предприятия;
- CVE – идентификация уязвимостей;
- CVSS – определение критичных уязвимостей;
- CCE – формирование наиболее защищенной конфигурации ИС;
- XCCDF – определение политики защищенной конфигурации;
- OVAL – оценка соответствия системы политике защищенной конфигурации;
- CWE – определение слабых мест РИС;
- CAPEC – определение атак относительно слабых мест РИС;
- CEE – определение событий для регистрации и параметров регистрации;
- ARF – объединение результатов оценки;
- MAEC – определение вредоносного ПО.

Следует отметить, что в NVD вычисляется индекс рабочей нагрузки на информацию I_W, который показывает количество критических уязвимостей. Чем выше число, тем больше нагрузка на систему безопасности. Индекс нагрузки NVD рассчитывается по следующей формуле:

$$I_W = (N_h + (N_m / 5) + (N_l / 20)) / 30,$$

где N_h, N_m и N_l – количество уязвимостей с высокой, средней и низкой степенью тяжести соответственно, которые были опублико-

ваны в течении последних 30 дней. Как видно из формулы одна уязвимость высокой степени тяжести приравнивается к пяти уязвимостям со средней и двадцати с низкой степенью тяжести [136]. На сайте NVD доступен полный список уязвимостей, содержащихся в базе, который отсортирован по годам и месяцам (см. рис. 1.30).

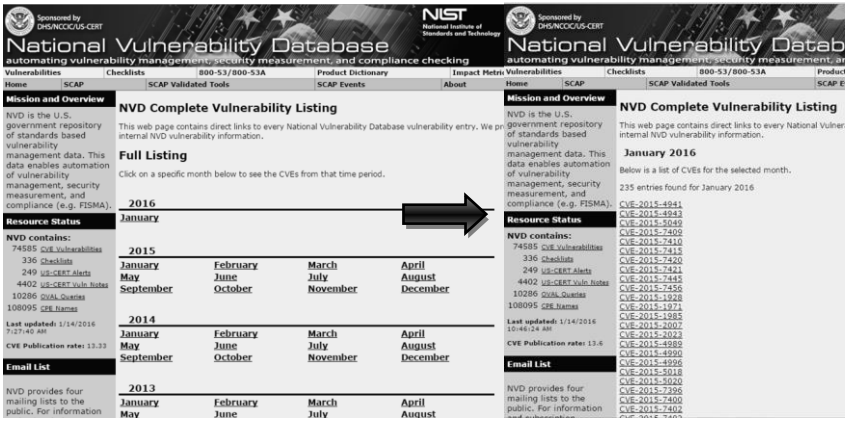


Рис. 1.30. Список уязвимостей на сайте NVD

Каждая уязвимость, вносимая в БД, описывается следующим набором параметров (рис. 1.31):

- уникальный CVE-идентификатор;
- даты внесения в БД;
- дата последней редакции;
- источник уязвимости (информации);
- краткое описание (обзор);
- результаты оценок по каждой метрической группе (МГ) CVSS (см. рис. 1.31, 1.32 и табл. 1.44) – базовой (Base Score), временной (Temporal Score) и контекстной (Environmental Score) (в БД CVSS доступен в двух версиях – v2.0 [142] и v3.0 [143]);
- уязвимые версии ПО;
- CWE категория;
- дополнительные ссылки;
- другие сведения [136].

National Cyber Awareness System

Vulnerability Summary for CVE-2015-4941

Original release date: 01/01/2016

Last revised: 01/05/2016

Source: US-CERT/NIST

Overview

IBM WebSphere MQ Light 1.x before 1.0.2 mishandles abbreviated TLS handshakes, which allows remote attackers to cause a denial of service (MQXR service crash) via unspecified vectors.

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Impact Score: 1.4

Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): None

Integrity (I): None

Availability (A): Low

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

**NOTE: Access Complexity scored Low due to insufficient information

Authentication: Not required to exploit

Impact Type: Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

External Source: CONFIRM

Name: http://www-01.ibm.com/support/docview.wss?uid=swg21972019

Type: Advisory

Hyperlink: http://www-01.ibm.com/support/docview.wss?uid=swg21972019

Vulnerable software and versions

+ Configuration 1
  + OR
    * cpe:/a:ibm:websphere_mq_light:1.0.0.1
    * cpe:/a:ibm:websphere_mq_light:1.0

* Denotes Vulnerable Software
Changes related to vulnerability configurations

Technical Details

Vulnerability Type (View All)

Code (CWE-17)

CVE Standard Vulnerability Entry http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4941

Change History 1 change record found - **show changes**

Рис. 1.31. Пример представления уязвимости в NVD

Отметим, что условие существования уязвимости хранится в виде дизъюнктивной нормальной формы. Рассмотрим более детально каждую из версий CVSS и определим их отличия.

CVSS v2.0.

Метрики и их параметры, входящие в стандарт CVSS v2.0 [142] показаны на рис. 1.32.

В этой версии осуществляется стандартизированное оценивание уязвимостей, система является открытой и ориентирована она определение приоритетных рисков.

Таблица 1.44. Значения показателей оценок CVSS v2.0

МГ	Множество показателей	Наборы символьных значений показателей	Числовые значения соответствующих показателей
Базовая	**AV**	L; A; N	0,395; 0,646; 1
	AC	H; M; L	0,35; 0,61; 0,71
	Au	M; S; N	0,45; 0,56; 0,704
	C; I; A	N; P; C	0; 0,275; 0,66
Временная	**E**	ND; U; POC; F; H	1; 0,85; 0,9; 0,95; 1
	RL	ND; OF; TF; W; U	1; 0,87; 0,9; 0,95; 1
	RC	ND; UC; UR; C	1; 0,90; 0,95; 1
Среды окружения	**CDP**	ND; N; L; LM; MH; H	0; 0; 0,1; 0,3; 0,4; 0,5
	TD	ND; N; L; M; H	1; 0; 0,25; 0,75; 1
	CR; IR; AR	ND; L; M; H	1; 0,5; 1; 1,51

Каждая МГ определяет характеристики уязвимости. Опишем эти группы (см. рис. 1.32).

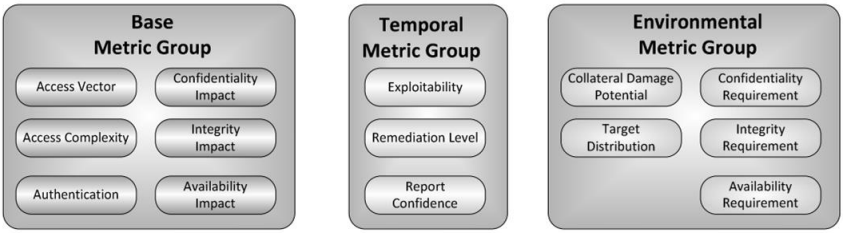


Рис. 1.32. МГ CVSS v2.0

Base Score Metrics (метрики базовых оценок) – характеристики уязвимостей, являющиеся постоянными в течение большого периода времени в пользовательских средах и не зависящие от них. Также они описывают сложность эксплуатации уязвимости и потенциальный ущерб для конфиденциальности, целостности и доступности. Используемые МГ состоят из следующих показателей:

- вектор доступа (Access Vector (**AV**));
- сложность доступа (Access Complexity (**AC**));
- аутентификация (Authentication (**Au**));
- воздействие на конфиденциальность (Confidentiality Impact (**C**));

- воздействие на целостность (Integrity Impact (**I**));
- воздействие на доступность (Availability Impact (**A**)).

Temporal Score Metrics (метрики временных оценок) – характеристики уязвимости, которые изменяются с течением времени, вне пользовательских сред. Они вносят в общую оценку поправку на полноту имеющейся информации об уязвимости, зрелость эксплуатируемого кода (при его наличии) и доступность исправлений. Ее показатели:

- возможность использования (Exploitability (**E**));
- уровень исправления (Remediation Level (**RL**));
- достоверность отчета (Report Confidence (**RC**)).

Environmental Score Metrics (метрики контекстных оценок) – характеристики уязвимости, которые актуальны и уникальны для среды конкретного пользователя. При помощи этих метрик эксперты по безопасности могут внести в результирующую оценку поправки с учетом характеристик информационной среды. Группа МГ состоит из показателей общих модификаторов (General Modifiers) –

- возможность косвенного ущерба (Collateral Damage Potential (**CDP**));
- целераспределение (Target Distribution (**TD**));

а также модификатори влияющих показателей (Impact Subscore Modifiers):

- требование конфиденциальности (Confidentiality Requirement (**CR**));
- требование целостности (Integrity Requirement (**IR**));
- требование доступности (Availability Requirement (**AR**)).

В таблице 1.44. для каждой МГ (метрикам оценок) по каждому множеству показателей приведены наборы символьных значений и соответствующие им числовые показатели. Здесь, каждому символьному значению определена соответствующая ему лингвистическая интерпретация:

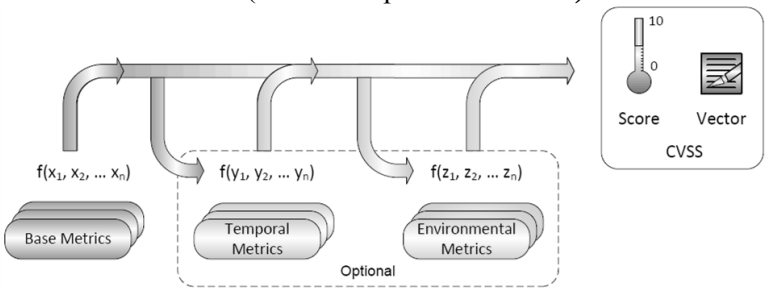
– для **AV** (Access Vector – вектор доступа):
  - L – «Локальный доступ»,
  - A – «Сопряженная сеть»,
  - N – «Сеть»;
- для **AC** (Access Complexity – сложность доступа):

- H – «Высокая»,
- M – «Средняя»,
- L – «Низкая»;

- для **Au** (Authentication – аутентификация):
  - M – «Многоразовая»,
  - S – «Одноразовая»,
  - N – «Отсутствует»;
- для **C** (Confidentiality Impact – воздействие на конфиденциальность), **I** (Integrity Impact – воздействие на целостность) та **A** (Availability Impact – воздействие на доступность):
  - N – «Отсутствует»,
  - P – «Частичное»,
  - C – «Полное»;
- для **E** (Exploitability – возможность использования):
  - ND – «Не определенна»,
  - U – «Теоретическая (нет доказательств)»,
  - POC – «Экспериментальная»,
  - F – «Функциональная»,
  - H – «Высокая»;
- для **RL** (Remediation Level – уровень исправления):
  - ND – «Не определен»,
  - OF – «Официальный патч»,
  - TF – «Временное решение»,
  - W – «Решение на основе советов и рекомендаций»,
  - U – «Отсутствует»;
- для **RC** (Report Confidence – достоверность отчета):
  - ND – «Не определенна»,
  - UC – «Носит предположительный характер»,
  - UR – «Не проработана»,
  - C – «Подтверждена»;
- для **CDP** (Collateral Damage Potential – возможность косвенного ущерба):
  - ND – «Не определенна»,
  - N – «Отсутствует»,
  - L – «Низкая»,
  - LM – «Низко – средняя»,

- MH – «Средне – высокая»,
- H – «Высокая»;

- для **TD** (Target Distribution – целераспределение):
  - ND – «Не определено»,
  - N – «Отсутствует»,
  - L – «Низкое»,
  - M – «Среднее»,
  - H – «Высокое»;
- для **CR** (Confidentiality Requirement – требование конфиденциальности), **IR** (Integrity Requirement – требование целостности) та **AR** (Availability Requirement – требование доступности):
  - ND – «Не определено»,
  - H – «Высокое»,
  - M – «Среднее»,
  - L – «Низкое» (также см. рис. 1.32 и 1.33).



Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Рис. 1.33. CVSS v2.0 – МГ и вектора

После присвоения символьным значениям конкретных чисел, осуществляется вычисление рейтинга (в приделах [0; 10]) и создание вектора (как показано на рис. 1.31) AV:N/ AC:L/ Au:N/ C:N/ I:N/ A:P, который отображает «открытость» структуры. Фактически, это текстовая строка, которая содержит значения, присвоенные каждой метрике и используется для взаимодействия оценок. Отме-

тим, что таким образом, вектор должен отображаться с учетом уязвимости [142]. Временные и контекстные МГ опциональны и применяются для более точной оценки опасности, которую представляет данная уязвимость для конкретной инфраструктуры. Значение МГ отображается в виде пары (см. рис. 1.33) из вектора (конкретные значения отдельных показателей) и числового значения, рассчитанного на основе всех показателей посредством формул стандарта [142].

Использование Temporal позволяет объединить временные и базовые показатели, отображаемые на шкалу с пределами [0; 10]. При этом временная оценка будет не выше базовой, но не меньше ее на 33% [142]. На рис. 1.34 показан встроенный калькулятор показателей CVSS v2.0 в Веб-интерфейс NVD [136].

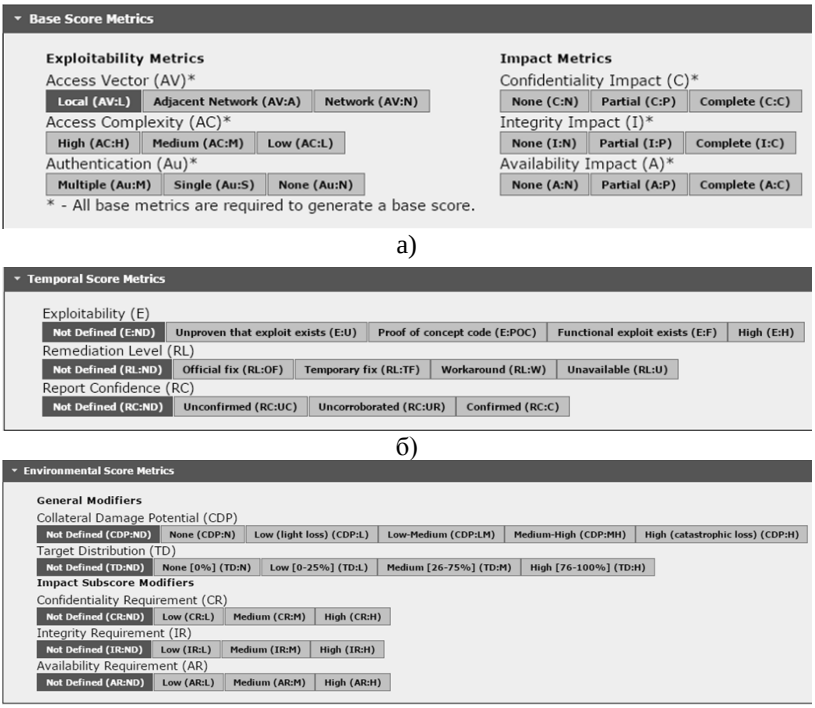


Рис. 1.34. Интерфейс встроенного калькулятора CVSS v2.0 в Веб-интерфейс NVD МГ: а) Базовая, б) Временная, в) Среды окружения

CVSS v3.0.

Калькулятор CVSS v3.0 является развитием CVSS v2.0. На рис. 1.35 в виде примера, схематически показаны изменения, внесенные в третью версию.

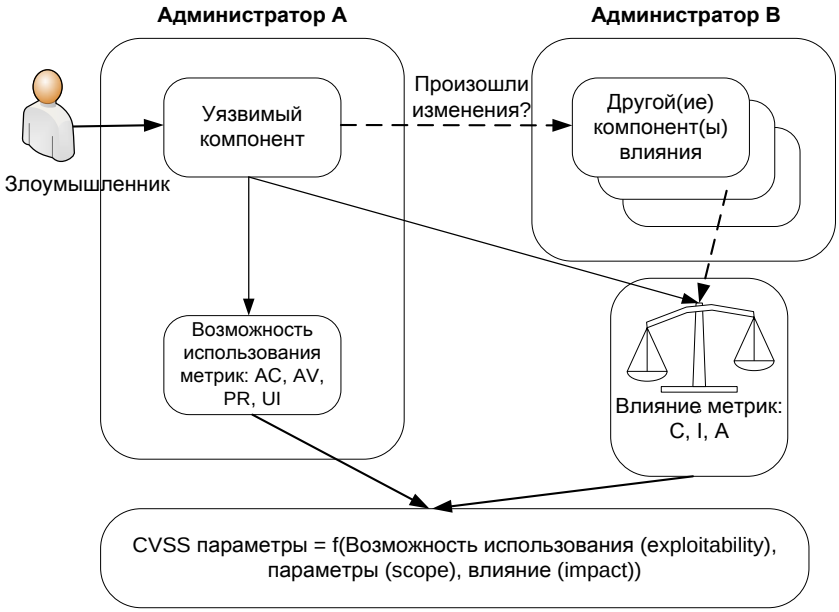


Рис. 1.35. Изменения в CVSS v3.0

Например, рассмотрим уязвимость в виртуальной машине, подвергающую угрозе основную операционную систему (ОС). Здесь уязвимым компонентом является виртуальная машина, а влияющим компонентом – ОС хоста. Это связано с тем, что эти два компонента независимо управляют правами на вычислительные ресурсы. Виртуальная машина (как показано на рис. 1.35) управляется «Администратором А», в то время как ОС хоста управляется «Администратором В». Когда два администратора одновременно эксплуатируют компоненты, то это может инициировать создание уязвимости. В этом случае CVSS считает, что изменения уже произошли. Это условие теперь отражается в новых МГ [143].

В рамках стандарта вводятся два следующих базовых понятия:

− уязвимый компонент (vulnerable component) – компонент ИС, содержащий уязвимость и участвующий в процессе эксплуатации;

− атакуемый компонент (impacted component) – компонент ИС, базовые характеристики безопасности которого (конфиденциальность, целостность, доступность) могут быть нарушены при успешной реализации атаки.

Как правило, уязвимый и атакуемый компоненты совпадают, но существуют классы уязвимостей, для которых это правило не работает, например:

− выход за пределы «песочницы» приложения;

− получение доступа к пользовательским данным, сохраненным в браузере, через уязвимость в Веб-приложении (XSS);

− выход за пределы гостевой виртуальной машины и др.

В этой версии метрики эксплуатируемости рассчитываются для уязвимого компонента, а метрики воздействия для атакуемого. Версия CVSS v2 не позволяла отображать ситуацию, при которой уязвимый компонент и атакуемый различаются [143, 144].

В CVSS v3.0 вектор доступа (Access Vector в v2.0) был переименован в вектор атаки, но, как и ранее, отражает «удаленность» злоумышленника по отношению к уязвимым компонентам. Другими словами, чем более отдаленным злоумышленник является относительно уязвимого компонента (с точки зрения логической и физической удаленности сети), тем больше будет базовая оценка. Кроме того, этот показатель различает локальные атаки, которые требуют локального доступа к системе (например, атака на прикладное приложение) и физические, которые требуют физического доступа к платформе для использования уязвимости (например, с FireWire, USB или jailbreaking атака) [142].

Изменения коснулись понятия значения показателя «Local», которое ранее описывало любые действия, не затрагивающие сеть. В новом стандарте вводится следующее деление значений этого показателя:

− Local (для эксплуатации атакующему требуется локальная сессия или определенные действия со стороны легитимного пользователя).

− Physical (атакующему требуется физический доступ к уязвимой подсистеме [142]).

Также изменения коснулись и показателя **AC** т.е. сложность эксплуатации уязвимости, представляющего собой качественную оценку сложности проведения атаки. Чем больше условий должно быть соблюдено для эксплуатации уязвимости – тем выше сложность [142]. Здесь были объединены два значения показателя «Low» и «Medium». Таким образом, сложность доступа была представлена в двух параметрах – сложность атаки и взаимодействие пользователя [143]. Понятие «сложность» само по себе субъективное, поэтому данный параметр, всегда трактовался экспертами поразному. Например, для уязвимостей, позволяющих реализовать атаку «Человек посередине» (активная атака [142]) в базе NVD можно встретить различные варианты оценки **AC**.

Теперь, для облегчения толкования данного параметра предлагаются только две ступени сложности «High» и «Low», а также более четко прописаны критерии отнесения к ним уязвимостей. В частности, уязвимость, позволяющую реализовать активную атаку, предписано относить к значению показателя «High». Факторы, учитываемые в CVSS v2 параметром **AC**, в новом стандарте раскрывается двумя показателями – Attack Complexity и User Interaction [144].

В CVSS v3.0 появился новый показатель «необходимые привилегии» (Privileges Required) заменяющий показатель «аутентификации» в v2.0 (аутентификация/требуемый уровень привилегий – требуется ли аутентификация для проведения атаки, и если требуется, то какая именно [144]). Необходимые привилегии, отражают уровень доступа, требуемый для успешной атаки. В частности, значения показателей «High», «Low» и «None» отражают привилегии, необходимые злоумышленнику для того, чтобы воспользоваться уязвимостью. Подход к расчету показателя, основан на количестве независимых процессов аутентификации, которые нужно пройти атакующему [144]. Все другие изменения в CVSS v3.0 отражены в таблице 1.45 [143]. Здесь, по аналогии с табл. 1.44, для каждой МГ по каждому множеству показателей приведены наборы символьных значений и соответствующие им числовые показатели.

Таблица 1.45. Значения показателей оценок CVSS v3.0

МГ	Множество показателей	Наборы символьных значений показателей	Числовые значения соответствующих показателей
Базовая	**AV**	N; A; L; P	0,85; 0,62; 0,55; 0,2
	AC	H; L	0,77; 0,44
	PR	H; L; N	0,85; 0,62 (или 0,68*); 0,27 (или 0,50*)
	UI	N; R	0,85; 0,62
	S	U; C	-
	C; I; A;	N; L; H;	0; 0,22; 0,56
Временная	**E**	U; P; F; H; X	0,91; 0,94; 0,97; 1; 1
	RL	O; T; W; U; X	0,95; 0,96; 0,97; 1; 1
	RC	U; R; C; X	0,92; 0,96; 1; 1
Среды окружения	**CR; IR; AR**	L; M; H; X	0,5; 1; 1,5; 1
Модифицированная базовая	**MAV; MAC; MPR; MUI; MS; MC; MI; MA**	Имеют те же символьные и числовые значения показателей, что и соответствующие не модифицированные показатели в базовой МГ, а также «Not Defined» (по умолчанию)	
*если область действия (S)/модифицированная область действия (MS) изменяется			

Кроме этого каждому символьному значению определена соответствующая ему лингвистическая интерпретация:

– для **AV** (Attack Vector – вектор атаки):
  - N – «Сеть»,
  - A – «Сопряженная сеть»,
  - L – «Локальный доступ»,
  - P – «Физический доступ»;
- для **AC** (Attack Complexity – сложность атаки):
  - H – «Высокая»,
  - L – «Средняя»;
- для **PR** (Privileges Required – необходимые полномочия):
  - H – «Высокие»,
  - L – «Средние»,
  - N – «Отсутствуют»;

- для **C** (Confidentiality Impact – воздействие на конфиденциальность), **I** (Integrity Impact – воздействие на целостность) и **A** (Availability Impact – воздействие на доступность):
  - H – «Высокое»,
  - L – «Среднее»,
  - N – «Отсутствует»;
- для **UI** (User Interaction – взаимодействие с пользователем):
  - N – «Отсутствует»,
  - R – «Требуется»;
- для **S** (Scope – область действия):
  - U – «Без изменений»,
  - C – «Изменена»;
- для **E** (Exploitability – возможность использования):
  - U – «Теоретическая (нет доказательств)»,
  - P – «Экспериментальная»,
  - F – «Функциональная»,
  - H – «Высокая»,
  - X – «Не определена»;
- для **RL** (Remediation Level – уровень исправления):
  - O – «Официальный патч»,
  - T – «Временное решение»,
  - W – «Решение на основе советов и рекомендаций»,
  - U – «Отсутствует»,
  - X – «Не определен»;
- для **RC** (Report Confidence – достоверность отчета):
  - U – «Отсутствует»,
  - R – «Обоснована»,
  - C – «Подтверждена»,
  - X – «Не определена»;
- для **CR** (Confidentiality Requirement – требование конфиденциальности), **IR** (Integrity Requirement – требование целостности) та **AR** (Availability Requirement – требование доступности):
  - L – «Низкое»,
  - M – «Среднее»,
  - H – «Высокое»,

− X – «Не определено».

Модифицированная базовая группа метрик описывается показателями:

MAV (Modified Attack Vector – модифицированный вектор атаки),

MAC (Modified Attack Complexity – модифицированная сложность атаки),

MPR (Modified Privileges Required – модифицированные необходимые полномочия),

MUI (Modified User Interaction – модифицированное взаимодействие с пользователем),

MS (Modified Scope – модифицированная область действия),

MC (Modified Confidentiality – модифицированная конфиденциальность),

MI (Modified Integrity – модифицированная целостность) и

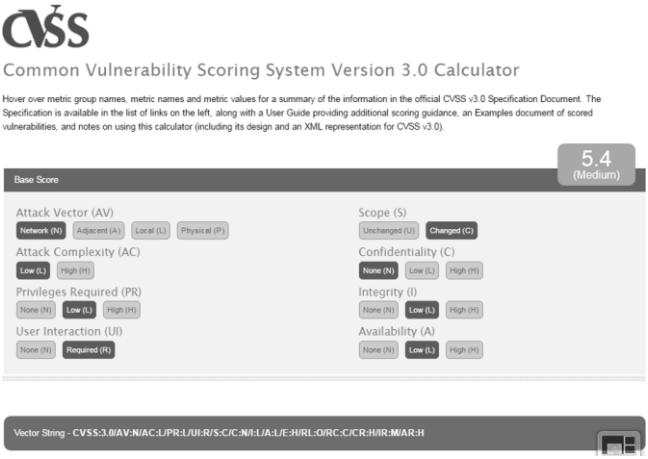
MA (Modified Availability – модифицированная доступность) (также см. рис. 1.35 и 1.36).

На рис. 1.36 показан встроенный калькулятор показателей CVSS v3.0 в Веб-интерфейс.

Рассмотрим примеры получения значений по уязвимости CVE-2015-1098 (Apple и Work Denial of Service Vulnerability) с помощью CVSS v2.0 и CVSS v3.0 (см. табл. 1.46) [143].

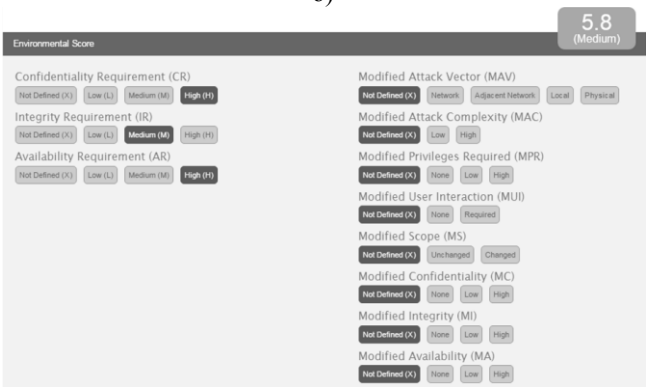
Таблица 1.46. Пример вычисления CVSS

Показатель		**Значение показателя**		**Числовое значение**	
v2.0	v3.0	v2.0	v3.0	v2.0	v3.0
AV		N	L	1	0,55
AC		M	L	0,61	0,44
Au	PR	N	N	0,704	0,27
-	UI	-	R	-	0,62
-	S	-	U	-	-
C		P	H	0,275	0,56
I		P	H	0,275	0,56
A		P	H	0,275	0,56
Результаты CVSS для базовой МГ				6,8	7.8



а)

б)



в)

Рис. 1.36. Интерфейс встроенного калькулятора CVSS v3.0 МГ: а) Базовая; б) Временная; в) Среды окружения

Согласно установленным правилам каждой уязвимости присваивается CWE категория, в соответствие с которым осуществляется группирование их по определенным категориям, отображающим так называемые слабые места РИС. Например, как показано на рис. 1.31, рассматриваемой уязвимости присвоена категория CWE-17, а на рис. 1.37 отображено описание этого кода. Согласно представленному на сайте CWE™ отчету на 07.12.2015 г. зафиксировано 1004 CWE категорий слабых мест [145].

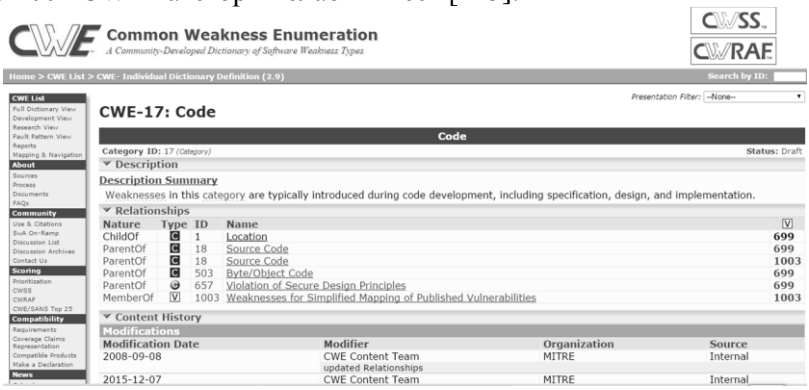


Рис. 1.37. Описание категории CWE-17

Пример описания уязвимостей доступных для скачивания в БД NVD показан в таблице 1.47. Здесь отображены уязвимости с идентификаторами CVE-2015-0001 – «Windows Error Reporting Security Feature Bypass Vulnerability» и CVE-2015-0032 – «VBScript Memory Corruption Vulnerability».

В представленной таблице каждому столбцу присвоен номер, который отражает, например, следующую информацию об уязвимостях в БД:

1 – версия базы данных;
2 – дата публикации;
3, 4 – идентификатор угрозы;
11 – название продукта;
12 – CVE-идентификатор угрозы;
14 – дата последнего изменения;
15 – оценка CVSS (см. рис. 1.38);
16 – вектор доступа;

Таблица 1.47. Пример описания уязвимостей

nvd_xml_version	pub_date	id	id2	operator	negate	name	operator3	negate4	name5	ns3:product	ns3:cve-id	ns3:published-datetime	ns3:last-modified-datetime	ns4:score	ns4:access-vector	ns4:access-complexity	ns4:authentication	ns4:confidentiality-impact	ns4:integrity-impact	ns4:availability-impact	ns4:source	ns4:generated-on-datetime	id6	ns2:lang	reference_type	ns3:source	ns3:reference	Href	ns2:lang7	ns3:summary	ns3:security-protection
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	09.12.2015 3:00:00	CVE-2015-0001	http://www.nist.gov/	OR	False	cpe:/o:microsoft:windows_8:-	-	-	-	cpe:/o:microsoft:windows_server 2012:r2::~~~x64~~	CVE-2015-0001	2015-01-13T17:59:00.050-05:00	2015-01-14T16:50:51.080-05:00	6,9	LOCAL	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-10-30T13:42:24.787-04:00	CWE-264	en	VENDOR_ADVISORY	MS	MS15-006	http://technet.microsoft.com/security/bulletin/MS15-006	en	*1)	-
2	09.12.2015 3:00:00	CVE-2015-0032	http://nvd.nist.gov/	AND	False	-	OR	False	cpe:/a:microsoft:vbscript:5.6	cpe:/a:microsoft:vbscript:5.7	CVE-2015-0032	2015-03-11T06:59:01.290-04:00	2015-09-10T11:58:19.313-04:00	9,3	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-09-10T10:43:58.757-04:00	CWE-399	en	VENDOR_ADVISORY	MS	MS15-019	http://technet.microsoft.com/security/bulletin/MS15-019	en	*2)	-

*1) Компонент отчета об ошибках Windows (WER) в Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold, R2 и Windows RT Gold позволяет локальным пользователям обойти механизм защиты и прочитать содержимое в произвольных местах процесса-памяти за счет использования административных привилегий.

*2) vbscript.dll в Microsoft VBScript 5.6 ÷ 5.8, используемый с Internet Explorer 8 ÷ 11 и других продуктов, позволяет удаленному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) посредством созданного Веб-сайта.

17 – сложность доступа;

18 – аутентификация;

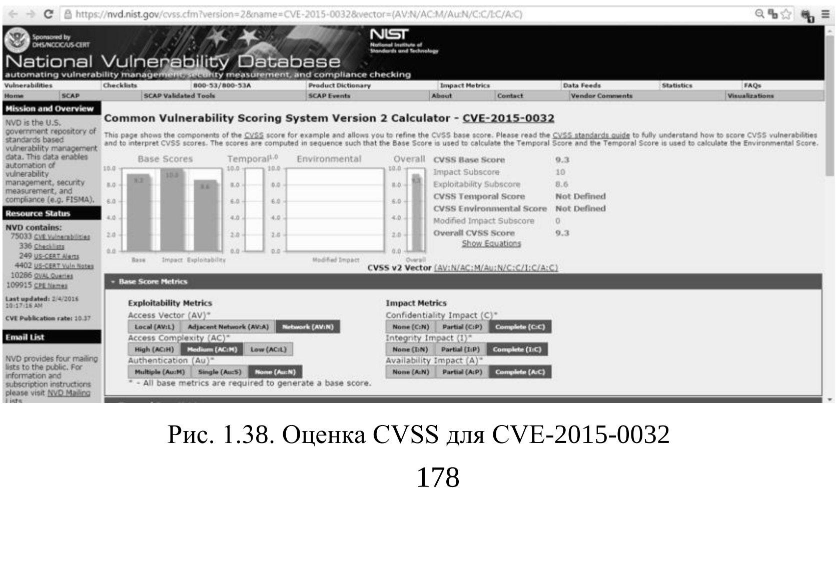


Рис. 1.38. Оценка CVSS для CVE-2015-0032

19, 20, 21 – соответственно воздействие на конфиденциальность, целостность и доступность;

22 – источник;

23 – время появления;

24 – CWE категория;

25 – язык;

26 – тип ссылки;

30 – язык (описание по заданному адресу);

31 – резюме и др. (см. табл. 1.47).

В ходе исследования базы NVD было установлено, что 82,77% уязвимостей принадлежат приложениям, 12,28% – ОС, а 3,59% – аппаратному обеспечению [132].

Банк данных угроз безопасности информации

Банк данных угроз безопасности информации (БДУБИ) разработан Федеральной службой по техническому и экспортному контролю России и Государственным научно-исследовательским испытательным институтом проблем технической ЗИ России.

Банк содержит сведения об основных угрозах ИБ и уязвимостях, в первую очередь, характерных для государственных ИС и автоматизированных систем управления производственными и технологическими процессами объектов критических инфраструктур.

Сведения об угрозах ИБ и уязвимостях ПО, содержащихся в БДУБИ, не являются исчерпывающими и могут быть дополнены по результатам анализа соответствующих угроз и уязвимостей в конкретной ИС с учетом особенностей ее эксплуатации. Данные, содержащиеся в БДУБИ не являются элементами иерархической классификационной системы и представляют собой обобщенный перечень основных угроз и уязвимостей ИБ (см. рис. 1.39) потенциально опасных для ИС. Последнее обновление БДУБИ от 11.07.16 г. содержало 186 угроз и 14395 уязвимостей [137].

Каждая угроза, вносимая в БДУБИ, описывается следующим набором параметров (рис. 1.39):

− уникальный идентификатор УБИ (угроза безопасности информации);

− наименование угрозы;

− описание угрозы;

– источник угрозы (тип нарушителя и его минимально необходимый функционал (потенциал)) (см. рис. 1.40);

– объект воздействия; последствия реализации угрозы [137].

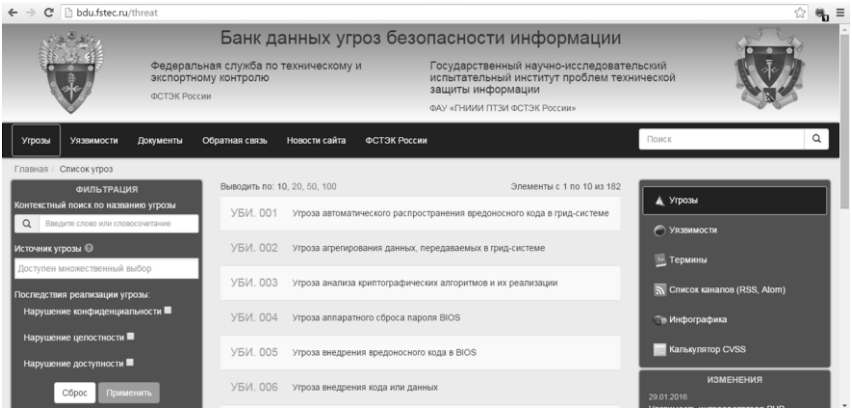


Рис. 1.39. Окно страницы описания угроз в БДУБИ

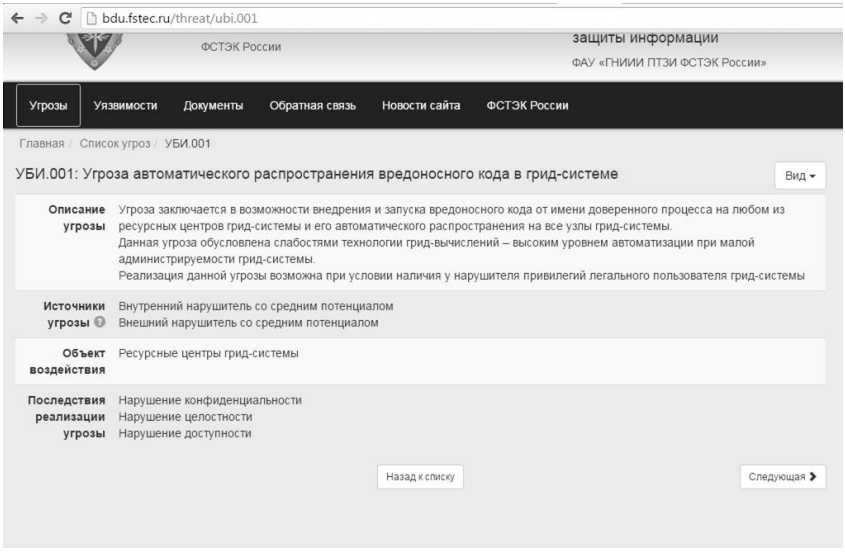


Рис. 1.40. Пример описания УБИ: 001

В процессе внесения в БДУБИ информации об уязвимостях используется следующий набор параметров (см. рис. 1.41):

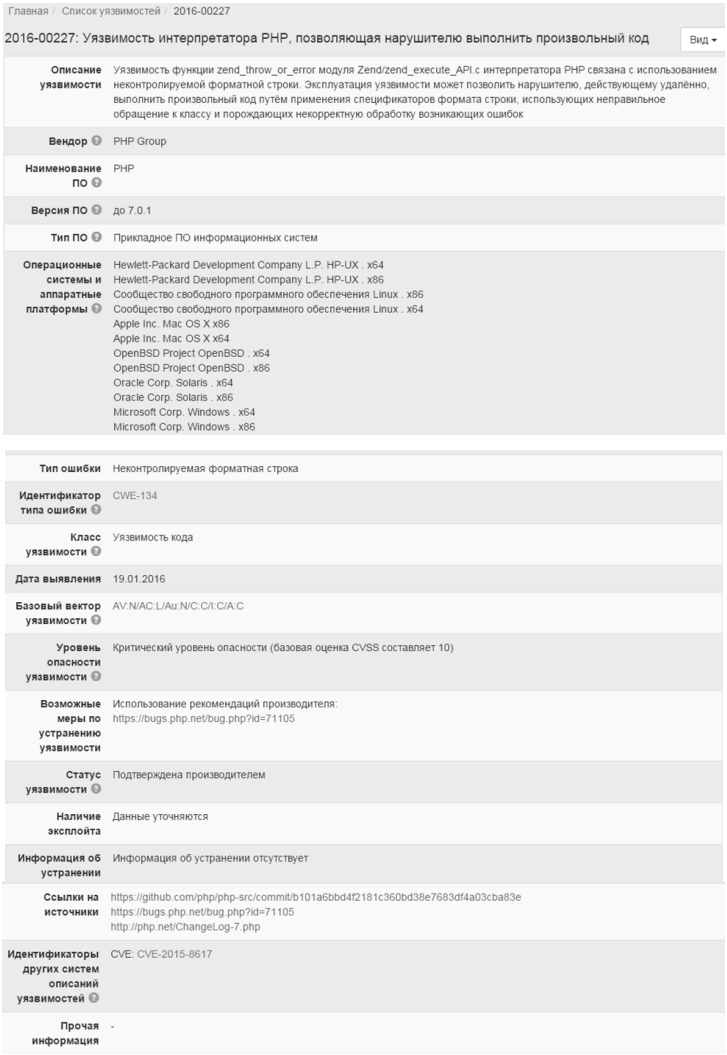


Рис. 1.41. Фрагмент примера описания уязвимости 2016-00227 в БДУБИ

– идентификатор (состоит из года и номера по порядку);

- наименование уязвимости;
- описание уязвимости;
- вендор (компания – производитель ПО в котором обнаружена уязвимость);
- название ПО;
- версия ПО;
- тип ПО;
- ОС и аппаратные платформы;
- тип ошибки;
- идентификатор типа ошибки (идентификатор, установленный в соответствии с общим перечнем ошибок CWE);
- класс уязвимости;
- дата выявления;
- вектор уязвимости базовой МГ (по CVSS v2.0);
- уровень опасности уязвимости (по CVSS v2.0);
- возможные меры по устранению уязвимости;
- статус уязвимости;
- наличие эксплойта;
- информация об устранении;
- ссылки на источники;
- идентификаторы других систем описаний уязвимостей (например, CVE);
- прочая информация [137] (см. таблицу 1.48).

Также на сайте БДУБИ содержится калькулятор CVSS v2.0 (см. рис. 1.42), являющийся русскоязычной версией аналогичного калькулятора NVD. Здесь представлена и инфографика, на которой отображены сводные данные по разным параметрам (рис. 1.43).

Open Sourced Vulnerability Database

Open Sourced Vulnerability Database (OSVDB). База создана OSVDB в 2002 году, как независимая и открытая БД уязвимостей для специалистов в области ИБ. Цель проекта состояла в том, чтобы обеспечить точную, детализированную и актуальную информацию об уязвимостях для систем обеспечения ИБ [133]. На 5 мая 2014 года данная база содержала 105413 уязвимостей. Веб-интерфейс OSVDB (см. рис. 1.44) не сильно отличается от базы NVD.

Таблица 1.48. Пример отчета по уязвимостям

1	№ п/п
Уязвимость микропрограммного обеспечения программируемого логического контроллера Schneider Electric Modicon Quantum, позволяющая злоумышленнику получить авторизованный доступ к устройству	**Наименование уязвимости**
2014-00001	**Открытый идентификатор уязвимости**
CVE-2011-4859	**Идентификаторы других систем описаний уязвимости**
Микропрограммное обеспечение модуля 140NOE77111 контроллера Schneider Electric Modicon Quantum содержит множество пар логин: пароль, установленных по умолчанию. Это позволяет любому пользователю, имеющему доступ к устройству по протоколу FTP, получить авторизованный доступ к устройству	**Описание уязвимости**
Микропрограммное обеспечение программируемого логического контроллера Schneider Electric Modicon Quantum	**Название ПО**
4.6	**Версия ПО**
Уязвимость архитектуры	**Класс уязвимости**
Микропрограммное обеспечение программируемого логического контроллера Schneider Electric Modicon Quantum (4.6)	**Наименование ОС и тип аппаратной платформы**
17.12.2011	**Дата выявления**
AV:N/AC:L/Au:N/C:C/I:C/A:C	**Базовый вектор CVSS**
Критический уровень опасности (базовая оценка CVSS составляет 10)	**Уровень опасности уязвимости**
Ограничение доступа к устройству по протоколу FTP	**Возможные меры по устранению**
Подтверждена производителем	**Статус уязвимости**
Существует	**Наличие эксплойта**
Информация об устранении отсутствует	**Информация об устранении**
http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-020-03	**Ссылки на источники**
Schneider Electric	**Вендор ПО**
Язык разработки ПО – C	**Прочая информация**
Жесткое кодирование паролей	**Описание ошибки CWE**
CWE-259	**Тип ошибки CWE**

Каждая уязвимость, заносимая в OSVDB, описывается следующими записями:

- идентификатор OSVDB;
- дата обнаружения;
- имя производителя;
- имя продукта;
- версия продукта (символьное значение), имеющего данную уязвимость;
- ссылка, указывающая на прямой адрес Интернет-ресурса другой базы или базы производителя, в которой описывается данная уязвимость;
- решение, имеющее описание «исправления» уязвимости;

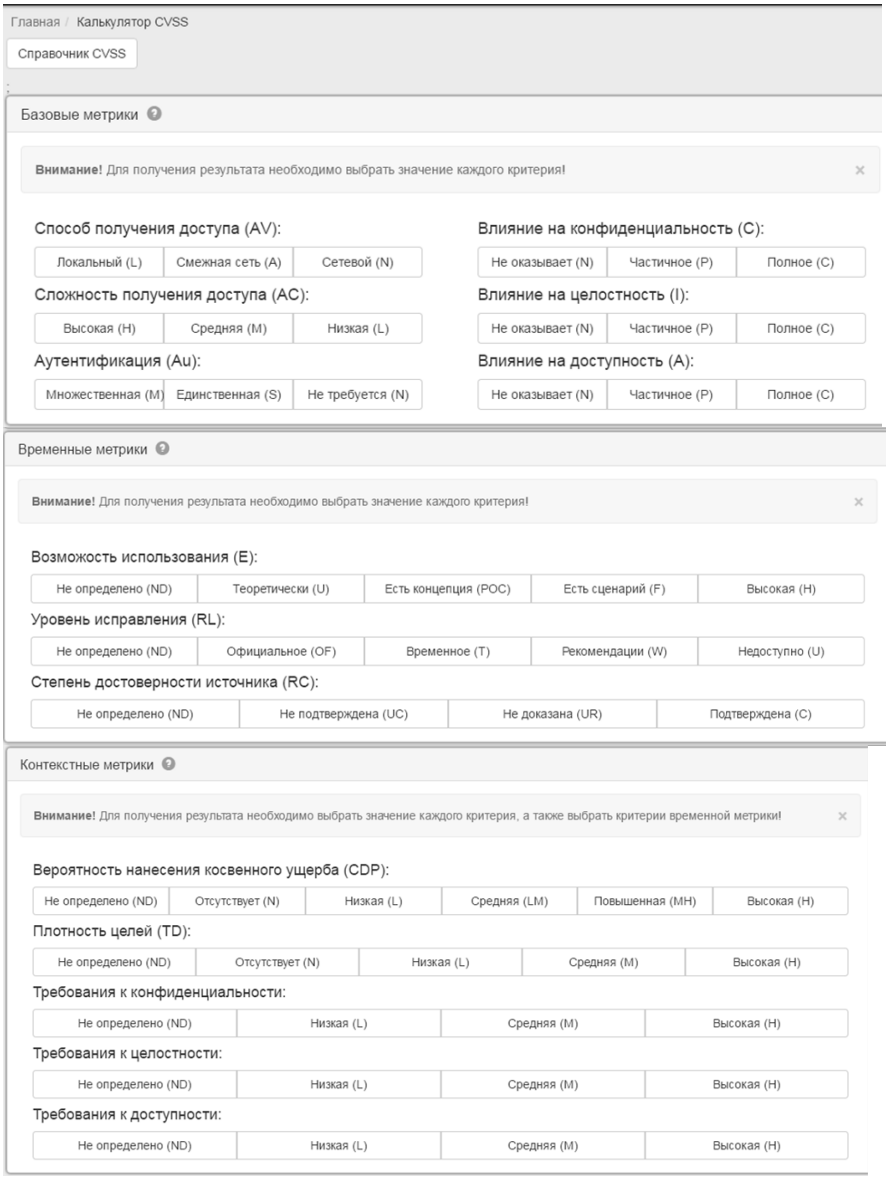


Рис. 1.42. Интерфейс калькулятора CVSS v2.0 на сайте БДУБИ

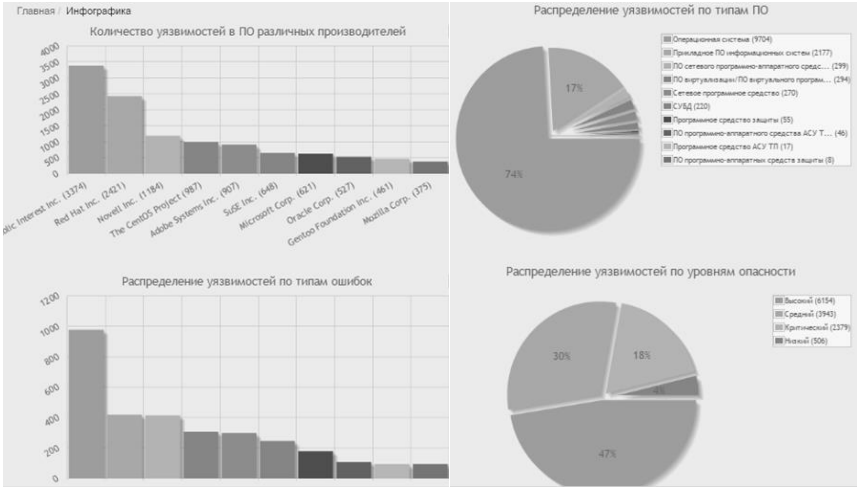


Рис. 1.43. Инфографика БДУБИ

− метрики уязвимости, содержащие критерии оценки уязвимостей в формате CVSS v2.0 (не являются обязательными ввиду того, что поле присутствует при наличии ссылки на базу NVD) [133, 138].

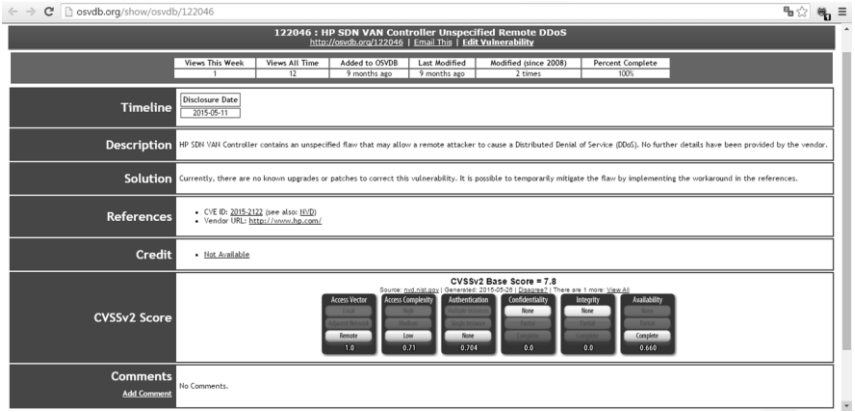


Рис. 1.44. Интерфейс OSVDB

Стоит отметить, что OSVDB с 2016 года стала условно открытой БД и теперь предоставляются платные услуги по информации

об уязвимостях. При этом, ее разработчики заключили сотрудничество с компанией Risk Based Security, которая продает клиентам лицензии на получение доступа к данным.

База данных уязвимостей IBM X-Force

База данных уязвимостей IBM ISS (Internet Security Services) X-Force, созданная специалистами подразделения IBM Internet Security Systems X-Force, является одной из самых больших и авторитетных БД в отрасли. Она содержит свыше 30000 записей и подробный анализ каждой известной уязвимости, обнаруженной с 1994 года.

Более того, специалисты подразделения X-Force сотрудничают с тысячами крупнейших в мире компаний и государственных учреждений, центрами анализа и вертикального обмена информацией (ISAC), глобальными координационными центрами и другими поставщиками решений [146].

Для доступа к БД уязвимостей необходимо пройти регистрацию на сайте IBM X-Force Exchange. После регистрации в строке поиска необходимо задать нужную информацию об уязвимости (см. рис. 1.45).

Как видно с описания уязвимости на рис. 1.45 используются, по аналогии с предыдущими базами, оценки CVSS (до 2016 года использовалась v2.0, после – v3.0), идентификатор CVE, краткое описание, дата создания отчета об уязвимости, затронутые продукты в которых есть эта уязвимость и внешние ссылки.

Но в отличие от других БД здесь присутствует поле «Последствия», выражающее в формализованном виде возможный результат эксплуатации уязвимости, например, «Gain Access» (получение доступа) и «Исправление», где приведены варианты контрмер [132, 139].

База данных записей уязвимостей US-CERT

База данных VND (см. рис. 1.46) записей уязвимостей US-CERT принадлежит United States Computer Emergency Readiness Team (US-CERT). Она разработана совместно с Office of Cybersecurity and Communications (Управление кибербезопасности и коммуникаций), Department of Homeland Security (Департамент внутренней

безопасности), Software Engineering Institute (Инженерный институт ПО) и Carnegie Mellon University (Институт Карнеги-Мелоуна).

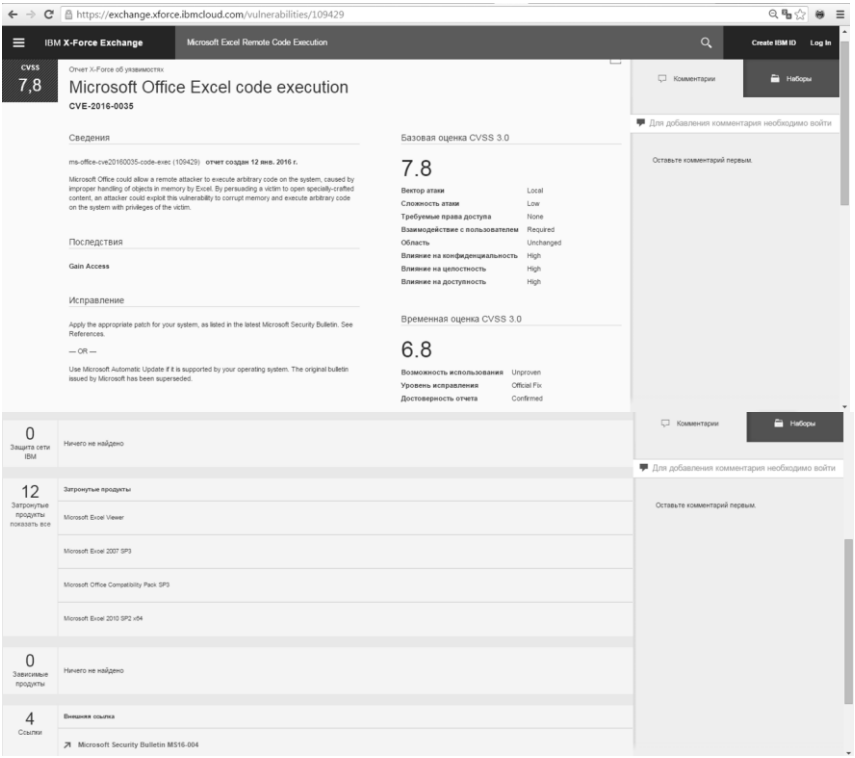


Рис. 1.45. Пример описания уязвимости Microsoft Excel Remote Code Execution

Каждой уязвимости в БД присваивается свой идентификатор «VU#», как показано на рис. 1.47 (VU#485744).

По аналогии с рассмотренными выше БД в VND присутствуют следующие основные пункты описания уязвимости:

- обзор;
- краткое описание;
- влияние;
- рекомендации об устранении;

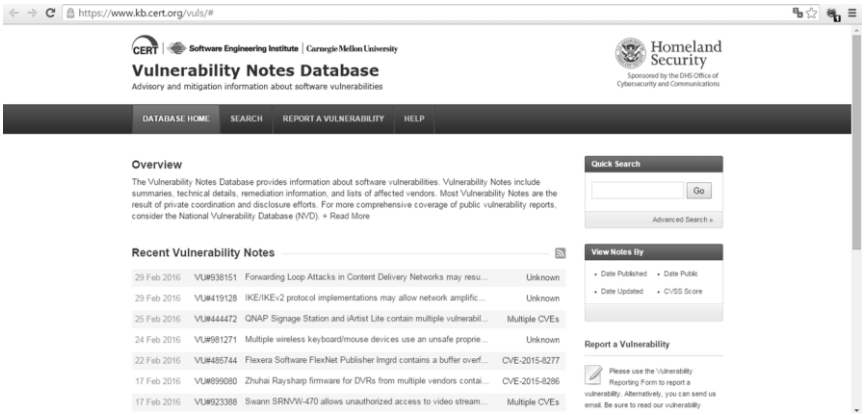
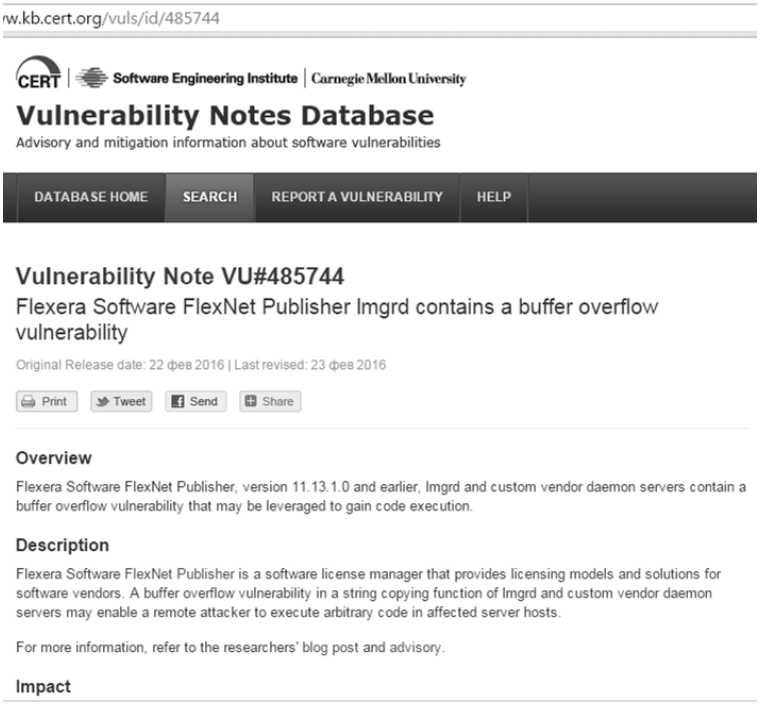


Рис. 1.46. Основная страница VND



A remote, unauthenticated attacker may be able to execute arbitrary code in affected server hosts.

Solution

Apply an update

Software vendors that distribute vulnerable lmgrd or vendor daemon components should obtain FlexNet Publisher 2015 (11.13.1.2) Security Update 1 or later from Flexera Software's Product and License Center. Users of affected software should contact product vendors for update information.

Vendor Information (Learn More)

Note that any vendor that distributes lmgrd or a customized version with their products may be affected. As the CERT/CC becomes aware of specific vendors and products, we will add them to the list below.

Vendor	Status	Date Notified	Date Updated
Flexera Software	Affected	-	22 Feb 2016

If you are a vendor and your product is affected, let us know.

CVSS Metrics (Learn More)

Group	Score	Vector
Base	10,0	AV:N/AC:L/Au:N/C:C/I:C/A:C
Temporal	7,8	E:POC/RL:OF/RC:C
Environmental	5,9	CDP:ND/TD:M/CR:ND/IR:ND/AR:ND

References

- http://learn.flexerasoftware.com/content/ECM-EVAL-FlexNet-Publisher
- https://flexerasoftware.flexnetoperations.com/control/inst/index
- http://securitymumblings.blogspot.com/2016/02/cve-2015-8277.html
- https://www.securifera.com/advisories/cve-2015-8277

Credit

Thanks to Matthew Benton, Ryan Wincey, and Richard Kelley for reporting this vulnerability.

This document was written by Joel Land.

Other Information

CVE IDs: CVE-2015-8277

Date Public: 22 фев 2016

Date First Published: 22 фев 2016

Date Last Updated: 23 фев 2016

Document Revision: 22

Feedback

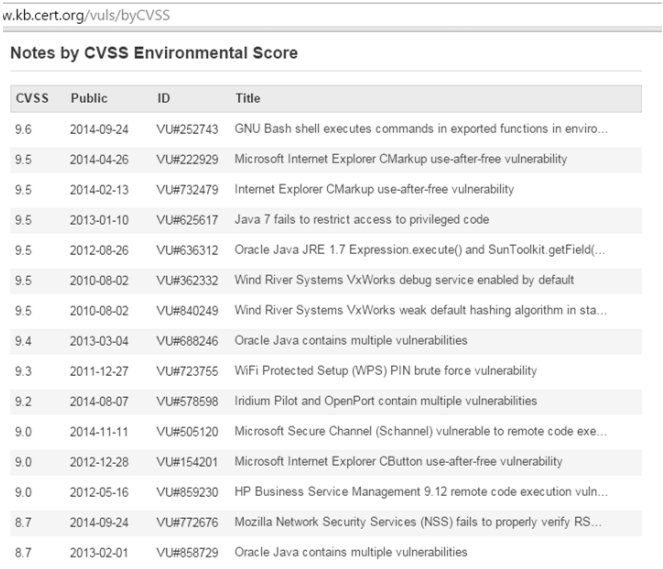
If you have feedback, comments, or additional information about this vulnerability, please send us email.

Рис. 1.47. Пример описания уязвимости

- оценки CVSS;
- также в дополнительной информации указывается (если есть) идентификатор CVE;

− дата первой публикации и обновления (см. рис. 1.48).

В отличие от остальных БД здесь уязвимости фиксируются с указанием пострадавшей стороны и информации о продавце. Так же на сайте БД VND присутствует возможность получения сводных данных оценок CVSS уязвимостей (см. рис. 1.48) [140].


w.kb.cert.org/vuls/byCVSS

Notes by CVSS Environmental Score

CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField(...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...
9.4	2013-03-04	VU#688246	Oracle Java contains multiple vulnerabilities
9.3	2011-12-27	VU#723755	WiFi Protected Setup (WPS) PIN brute force vulnerability
9.2	2014-08-07	VU#578598	Iridium Pilot and OpenPort contain multiple vulnerabilities
9.0	2014-11-11	VU#505120	Microsoft Secure Channel (Schannel) vulnerable to remote code exe...
9.0	2012-12-28	VU#154201	Microsoft Internet Explorer CButton use-after-free vulnerability
9.0	2012-05-16	VU#859230	HP Business Service Management 9.12 remote code execution vuln...
8.7	2014-09-24	VU#772676	Mozilla Network Security Services (NSS) fails to properly verify RS...
8.7	2013-02-01	VU#858729	Oracle Java contains multiple vulnerabilities

Рис. 1.48. Сводные данные оценок CVSS

База данных уязвимостей SecurityFocus

База данных уязвимостей SecurityFocus разработана в 1999 и принадлежит компании Symantec (рис. 1.49) [141]. В SecurityFocus при добавлении уязвимости последней присваивается Bugtraq ID и определяется класс (рис. 1.50).

По аналогии с другими открытыми БД уязвимость также имеет:

− свой идентификатор CVE;
− дату опубликования и обновления;
− информацию об удаленности или локальности;
− уязвимых продуктах.

На сайте для каждой уязвимости дополнительно размещена информация, в виде отдельных вкладок, обсуждение (описание), ин-

формация об использовании, решение о контрмерах и рекомендации (см. рис. 1.50).

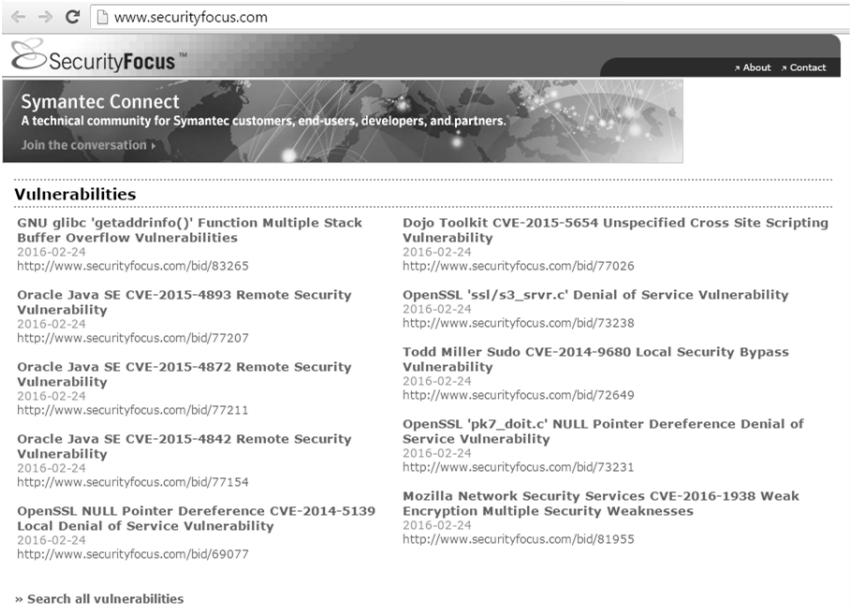


Рис. 1.49. Основная страница БД SecurityFocus

В результате проведенного исследования БД можно сделать выводы, что практически каждой уязвимости, вносимой в ту или иную базу, присваивается идентификатор CVE и определяется оценка CVSS.

Также во время исследования были определены критерии (см. таблицу 1.49), по которым можно реализовывать сравнение подобных БД.

К таким критериям относятся наличие:

- оценки CVSS по v2.0 и/или v3.0;
- калькулятора CVSS;
- идентификатора CVE;
- CWE категории;
- возможности расширения;
- вывода критических угроз/уязвимостей;

- возможности интеграции;
- оценки риска/риск-калькулятора.

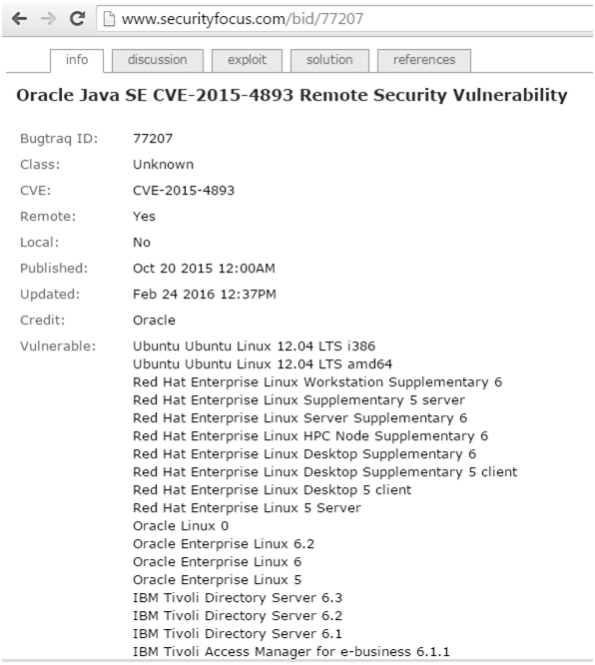


Рис. 1.50. Фрагмент окна с примером описания уязвимости Bugtraq 77270

Таблица 1.49. Сводные данные исследования БД уязвимостей

БД	Критерии									
	Оценка риска/ риск-калькулятор	Версии CVSS		Калькулятор CVSS		CVE идентификатор	CWE категория	Возможность расширения	Вывод критических угроз/ уязвимостей	Возможность интеграции
		v2.0	v3.0	v2.0	v3.0					
NVD	-	+	+	+	+	+	+	+	-	+
БДУБИ	-	+	-	+	-	+	+	+	-	-
OSVDB	-	+	-	-	-	+	-	-	-	+
IBM X-Force	-	+	+	-	-	+	+	+	-	+
VND	-	+	+	-	-	+	+	+	+	+
Security Focus	-	-	-	-	-	+	-	+	-	+

Приведенные критерии могут быть полезны разработчикам систем оценивания ИБ. Так же стоит отметить, что процедура оценивания риска не предусмотрена ни в одной из представленных БД.

Таким образом, определен набор критериев для БД уязвимостей РИС по которым можно осуществить сравнительный анализ таких баз и выбрать наиболее подходящие для построения различных средств оценивания состояния ИБ, например, систем оценивания рисков или риск-калькуляторов.

СПИСОК ЛИТЕРАТУРЫ К ГЛАВЕ 1

1. «Information technology. Security techniques. Information security management systems. Requirements», *ISO/IEC 27001:2013*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

2. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст]», *НД ТЗІ 3.7-003 – 2005*. Чин. 2005.11.08. – К. : ДСТСЗІ СБ України, 2005. – 12 с.

3. «Типове положення про службу захисту інформації в автоматизованій системі [Текст]», *НД ТЗІ 1.4-001–2000*, Чин. 2000.12.04, К.: ДСТСЗІ СБ України, 2000, с. 32.

4. М. Луцкий, А. Корченко, Е. Иванченко, С. Казмирчук, «Исследование программных средств анализа и оценки риска информационной безопасности», *Захист інформації*, №3, С. 97–108, 2011.

5. А. Качинський, «Аналіз ризику – методологічна основа для розв'язання проблем безпеки людини та довкілля», Серія "Екологічна безпека". *Екологічна безпека України. Системний аналіз перспектив покращення. Розділ 3*, К.: Національний інститут стратегічних досліджень, 2001. [Online]. Режим доступа: http://www.niss.gov.ua/book/Kachin/1-3.htm. [переглянуто 15 березня 2010].

6. В. Ахундов, А. Соболь, *Финансовый риск*, М.: Изд-во МСХА, 2000, с.128.

7. «Глоссарий» [Электронный ресурс] : *Служба тематических толковых словарей, руководитель проекта* С. Соловьев, редактор баз знаний Н. Казеннова, мастер семантической сети Г. Гинкул, [Online], Режим доступа: http://www.glossary.ru/. [просмотрено 25 апреля 2010].

8. А. Грицанов, «Новейший философский словарь» [Электронный ресурс], *Национальная философская энциклопедия*, Мн.: Национальная энциклопедическая служба, 1998, [Online], Режим доступа: http://terme.ru/dictionary/. [просмотрено 25 апреля 2010].

9. Е. Дзекцер, «Геологическая опасность и риск (методологическое исследование)», *Инженерная геология*, № 6, С. 3–10, 1992.

10. А. Захаров, «Информационные системы: оценка рисков», *Information Security (Информационная безопасность)*, №6, С. 18–19, 2005.

11. «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий», *ГОСТ Р ИСО/МЭК 13335-1*, 2006, Введ. 2007.05.31, М.: ИПК «Издательство стандартов», 2007, с. 23.

12. «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий = Information technology. Security techniques. Methodology for IT security evaluation», *ГОСТ Р ИСО/МЭК 18045,* 2008, Введ. 2008.12.18, М.: ИПК «Издательство стандартов», 2008, с. 234 .

13. «Информационная технология. Уровни целостности систем и программных средств», *ГОСТ Р ИСО/МЭК 15026,* 2002, Введ. 2003.06.30, М.: ИПК «Издательство стандартов», 2003, с. 15.

14. «Информационные технологии. Свод правил по управлению защитой информации», *ISO/IEC 27002:2005(E)*, М.: Компания «Технорматив», 2007, с.117.

15. В. Индеева, «К вопросу об определении понятия «риск» [Электронный ресурс], *заочных электронных конференций*, М.: Российская Академия Естествознания, 2009, [Online]. Режим доступа: http://www.rae.ru/zk/arj/2007/02/Indeeva.pdf. [просмотрено 20 апреля 2010].

16. М. Кондратьев, В. Ильин, *Азбука социального психолога-практика: Справочно-энциклопедическое издание*, М.: ПЕР СЭ, 2007, с.464.

17. В. Коноплицкий, А. Филина, Это – бизнес. *Толковый словарь экономических терминов*, К.: Издательство «Альтерпресс», 1996, с.184.

18. А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*, К.: МК-Пресс, 2006, с. 320.

19. Л. Лопатников, *Экономико-математический словарь, Словарь современной экономической науки*, 5-е изд., перераб. и доп., М.: Дело, 2003, с. 520.

20. В. Маршалл, *Основные опасности химических производств*, М.: Мир, 1989, с. 672.

21. «Менеджмент риска. Термины и определения», *ГОСТ Р 51897–2002*, Введ. 2001.05.31., М.: ИПК «Издательство стандартов2, 2002, с. 8.

22. Э. Мушик, П. Мюллер, *Методы принятия технических решений*, М.: Мир, 1990, с. 208.

23. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», *СТО БР ИББС 1.0, 2006*, Введ. 2006.01.01, М.: ИПК «Издательство стандартов», 2006, с. 27.

24. С. Ожегов, Н. Шведова, *Толковый словарь русского языка: 80 000 слов и фразеологических выражений, 4-е изд., дополненное*, М.: Азбуковник, 1999, с. 944. (Российская академия наук. Институт русского языка им. В.В. Виноградова).

25. «Оксфордский толковый словарь по психологии» [под. Ред. А. Ребера], Oxford: Penguin Non-Classic, 2002, с. 864.

26. «Охорона праці. Терміни та визначення основних понять», *ДСТУ 2293-99*, Чинний з 2000.01.01, К.: Держстандарт України, 1999, с. 22.

27. С. Петренко, С. Симонов, *Управление информационными рисками. Экономически оправданная безопасность*, М.: Компания АйТи, ДМК Пресс, 2004, с. 384.

28. «Про основні засади державного нагляду (контролю) у сфері господарської діяльності [Текст]» *Закон України №877-V* від 5 квітня 2007 р., Верховна Рада України, Відомості Верховної Ради України, 2007, №36, Ст. 389.

29. Ф. Рагозин, «Оценка и картографирование опасности и риска от природных и техногенных процессов (теория и методология)», *Проблемы безопасности при чрезвычайных ситуациях*, №5, С. 16–41, 1993.

30. Б. Райзберг, Л. Лозовский, Е. Стародубцева, *Современный экономический словарь*, 5-е изд., перераб. и доп., М.: Инфра-М, 2006, с.494.

31. «Риск» [Электронный ресурс], [Авторы Википедии], Версия 44986537, *Википедия, Свободная энциклопедия*, Сан-Франциско : Фонд Викимедиа, 2012. [Online]. Режим доступа: http://ru.wikipedia.org/?oldid=44986537. Описание на основе версии, датированной 3 июня 2012 08:54 UTC.

32. «Российская энциклопедия по охране труда», [В 3 т.], *2-е изд., перераб. и доп.*, М.: Изд-во НЦ ЭНАС, 2007, Т. 2, Л, Р, с. 408.

33. «Руководство по управлению рисками безопасности» [Электронный ресурс], *Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам*; Центр Microsoft security center of excellence, TechNet, Редмонд, США: Корпорация Майкрософт, 2006, [Online]. Режим доступа: http://technet.microsoft.com/ru-ru/library/cc163143.aspx. – [просмотрено 29 декабря 2011].

34. «Словарь по экономике и финансам. Глоссарий. Ру» [Электронный ресурс], *Яндекс: [интернет-портал]*, М.: Публичная компания «Яндекс», 2010, [Online]. Режим доступа: http://slovari.yandex.ru/dict/glossary. [просмотрено 19 декабря 2010].

35. «Социальная психология», под общей ред. Петровского А., редактор-составитель Карпенко Л., под ред. Венгер А., М.: ПЕР СЭ, 2005, с. 176.

36. «Стандартизация в Российской Федерации. Термины и определения = Standardization in the Russian Federation. terms and definitions», *ГОСТ Р 1.12 – 2004*, Введ. 2005.07.01, М.: ИПК «Издательство стандартов», 2004, с. 17.

37. «Страховой бизнес: словарь-справочник» [Электронный ресурс], *Международный Институт Исследования Риска*, М.: Международный Институт Исследования Риска, 2010, [Online]. Режим доступа: http://www.miir.ru. [просмотрено 20 мая 2010].

38. «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]», *НД ТЗІ 1.1-003 – 1999*, Чин. 1999. 04.28, К.: ДСТСЗІ СБ України, 1999, с. 12.

39. «Технологии анализа рисков» [Электронный ресурс], *Группа компаний «Компьюлинк», Электрон. дан*, М.: Группа

компаний «Компьюлинк», 2003, [Online]. Режим доступа: http://www.glossary.ru/. [просмотрено 25 марта 2010].

40. «Управление надежностью. Анализ риска технологических систем», *ГОСТ Р 51901 – 2002*, Введ. 2003.09.01., М. : ИПК «Издательство стандартов», 2002, с. 21.

41. J. Fiksel, «Quantitative risk analysis for toxic chemicals in the environment», *of hazard materials*, 10, № 2-3, P. 227–240, 1987.

42. S. Hill, M. Smith, «Risk Management & Corporate Security», *Computers & Security*, P. 199–204, 1995.

43. S. Lichtensteir, «Factors in the Selection of a Risk Assessment Method», *Information Management & Computer Security*, Vol. 4 Iss: 4, P. 20–25, 1993.

44. «Risk analysis based on IT-Grundschutz», *BSI-Standard 100-3*, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23.

45. «Risk Management Tools. Program Risk Management Tools» [Electronic resource], *The MITRE Corporation*. All rights reserved, New York: Solutions That Make a Difference, 2012, [Online]. Access mode: http://mitre.org/work/systems_ engineering/guide/ risk_ management_ tools.html.

46. «Risk management. Vocabulary», *ISO Guide 73:2009*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2002, p. 15.

47. M. Smith, *Commonsense Computer Security, your practical guide to information security*, London: McGraw, Hill, 1993, p. 105.

48. A. Syalim, Y. Hori, K. Sakurai, «Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide», *International Conference on Issue*, Fukuoka: Grad. Sch. of Inf. Sci. & Electr. Eng, P. 726–731.

49. «U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard», *United States Federal Register*, 42, №70, P. 14292–14296, 1977.

50. В. Кохановский, В. Яковлев, *История философии: Учебник для высших учебных заведений*, Ростов-на-Дону: Феникс, 2002, с. 576.

51. A. Taha, Hamdy, *Operations Research. An Introduction*, New York: MacMillan Publishing Company, 1987, p. 123.

52. В. Гранатуров, *Экономический риск: сущность, методы измерения, пути снижения*, М. : изд-во «Дело и Сервис», 1999, с. 112.

53. А. Корченко, Е. Иванченко, С. Казмирчук, «Определение понятия риска для сферы информационной безопасности», *Проблеми та перспективи розвитку транспортних систем в умовах реформування залізничного транспорту: управління, економіка і технології*: V міжнар. наук.-практ. конф. : тези доп., К.: ДЕТУТ, 2011, С. 255–256.

54. А. Корченко, Е. Иванченко, С. Казмирчук, «Анализ и определение понятия риска для его интерпретации в области информационной безопасности», *Захист інформації*, №3, С. 5–10, 2010.

55. О. Корченко, С. Казмірчук, Т. Сирота, «Визначення поняття ризику у сфері інформаційної безпеки», *Актуальні проблеми забезпечення інформаційної безпеки держави*: наук.-практ. конф. : тези доп., К.: Вид-во НА СБУ, 2011, С. 96–99.

56. В. В. Яременко, О. М. Сліпушко, *Новий тлумачний словник української мови*. [том 3], К.: Вид. «Аконіт», 2007, с 862.

57. А.Б. Качинський, *Безпека, загрози і ризик: наукові концепції та математичні методи*, К., 2003, с. 472.

58. Я.Д. Вишняков, Н.Н. Радаев, *Общая теория рисков*, М.: Изд. центр «Академия», 2008, с. 368.

59. А.В. Катренко, В.В. Пасічник, В.П. Пасько, *Теорія прийняття рішень*, К.: Видавнича група BHV, 2009, с.448: іл.

60. А.В. Шегда, М.В. Голованенко; за ред. А.В. Шегди, *Ризики в підприємництві: оцінювання та управління: навч. посіб.*, К.: Знання, 2008. с. 271.

61. В.М. Гранатуров, *Экономический риск: сущность, методы измерения, пути снижения*, М.: изд-во «Дело и Сервис», 1999, с. 112.

62. В.М. Гранатуров, *Экономический риск: сущность, методы измерения, пути снижения*, М.: изд-во «Дело и Сервис», 1999, с. 112.

63. В.В. Вітлінський, Г.І. Великоіваненко, *Ризикологія в економіці та підприємництві: Монографія*, К.: КНЕУ, 2004, с. 480.

64. І.Ю. Івченко, *Моделювання економічних ризиків і ризикових ситуацій*, К.: Центр учбової літератури, 2007, с. 344.

65. «Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ». *(ISO/IEC TR 13335–3) : ДСТУ ISO/IEC TR 13335–3*, (Чинний з 2004-10-01), К.: Держспоживстандарт України, 2005, ІІІ. с. 76, (Національний стандарт України).

66. «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки *(ISO/IEC 27005:2011, IDT)», ДСТУ ISO/IEC 27005:2015*, К.: ДП «УкрНДНЦ», 2016.

67. В.И. Соболев. *Информационно-статистическая теория измерений*, М.: Машиностроение, 1983, с. 224.

68. В.С. Пугачев, *Теория вероятности и математическая статистика*, М.: Наука, Главная редакция физико-математической литературы, 1979, с. 496.

69. О.Є. Архипов, І.П. Касперський, «Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, К, Вип.2 (15), С.13–19, 2007.

70. О.Є. Архипов, С.О. Носок, *Основи документаційного забезпечення діяльності організації. Навчальний посібник*. К.: НТУУ «КПІ», 2010.-НМУ № Е 10/11-084.

71. С.А. Айвазян, И.С. Енюков, Л.Д. Мешалкин, *Прикладная статистика: Основы моделирования и первичная обработка данных. Справочное изд.*, М.: Финансы и статистика, 1983, с. 471.

72. И.Г. Черноруцкий, *Методы принятия решений*, СПб.: БХВ-Петербург, 2005, с. 416.

73. М. Луцкий, Е. Иванченко, С. Казмирчук, «Базовые понятия управления риском в сфере информационной безопасности», *Захист інформації*, № 2, С. 86–94, 2011.

74. «International standard Risk management. Principles and guidelines», *ISO/FDIS 31000:2009(E)*, International Organization for Standardization, JISC, 2009, p. 24.

75. «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. II», *Catalogue of Elements*, [version

2], Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006, p. 87.

76. О. Ботвінкін, В. Шлапаченко, В. Ворожко, А. Пашков, *Історія охорони державної таємниці в Україні: монографія*, К.: Наук.-вид. відділ НА СБ України, 2008, с. 155.

77. Cal Jaeger, «Security Risk Assessment Methodology for Communities (RAM-C)», *Security Technology, International Carnahan Conference on* : onference Publications, New Mexico : Security Systems and Technology Center Sandia National Laboratories Albuquerque, P. 106–110, 2004.

78. «Словарь бизнес-терминов» [Электронный ресурс], *dic.academic*, Академик: М.: Академик, 2010. [Online]. Режим доступа: http://dic.academic.ru/dic.nsf/business/13134. [просмотрено 15 марта 2010].

79. W. Caelli, D. Longley, M. Shain, *Information Security for Managers. Information Security Handbook*, UK.: Stockton Press, 1989, p. 26.

80. А. Астахов, *Искусство управления информационными рисками*. М.: ДМК Пресс, 2010, с. 314.

81. Т. Бартон, У. Шенкир, П. Уокер, *Риск-менеджмент; пер. с англ.*, М.: Издательский дом «Вильямс», 2008, с. 208. (Практика ведущих компаний).

82. «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]», *National Institute of Standards and Technology Special Publication 800-30*, Falls Church: Natl. Inst. Stand. Technol, 2002, p. 54.

83. «Рекомендации в области стандартизации банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности», [Электронный ресурс], *РС БР ИББС-2.2-2009*, Введ. 2010.01.01, Банк России: Официальный сайт, М.: Банк России. [Online]. Режим доступа: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. [просмотрено 29 декабря 2011].

84. «Information Technology – Security techniques – Information security risk management *(ISO/IEC 27005:2008)», ISO/IEC JTC 1/SC 27*, 2008, p. 62.

85. «Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности», *BS ISO/IEC 27005:2008*, К.: 2011, с. 70.

86. М. Луцкий, Е. Иванченко, А. Корченко, С. Казмирчук, А. Охрименко, «Современные средства управления информационными рисками», *Захист інформації*, №1, С. 5–16, 2012.

87. А. Корченко, А. Архипов, С. Казмирчук, *Анализ и оценивание рисков информационной безопасности. Монография*, Киев: ООО «Лазурит-Полиграф», 2013, с. 275.

88. «Risk management», *Standard AS/NZS 4360:2004*, Nundah : ISO working group – risk management Terminology, 2004, p. 65.

89. Д.А. Марцынковский, «Обзор основных аспектов риск-менеджмента», № 1/11-12, С. 54–59, 2009.

90. Д.А. Марцынковский, «Обзор основных аспектов риск-менеджмента», *Компетентность*, № 1, С. 37 – 42, 2009.

91. В. Галатенко, *Стандарты информационной безопасности*, М.: Интернет-Университет Информационных технологий, 2004, с. 328.

92. С. Казмірчук, В. Волянська, «Дослідження методик оцінки ризиків», *Сучасні проблеми захисту інформації з обмеженим доступом*: міжвідомча науково-практ. конф., тези доп., К., С. 67–69, 2008.

93. P. Grant, «ISO 31000:2009, Setting a New Standard for Risk Management», *Risk Analysis*, Vol. 30, №6, P. 881 – 886, 2010.

94. А. Прилипко, «Новые стандарты серии ISO 31000 – Риск-менеджмент», [електронний ресурс], *Тренинговый портал Украины*, 2010, Режим доступу: http://trn.work.ua/articles/1750/.

95. Н.Є. Стрельбіцька, «Уніфікований міжнародний стандарт ризик-менеджменту як відповідь на виклики глобалізації», [Електронний ресурс], Соціально-економічні проблеми і держава, Вип. 2 (5). 2011. Режим доступу: http://sepd.tntu.edu.ua/images/stories/pdf/2011/11snynvh.pdf.

96. И. Медведовский, «Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ» [Электронный ресурс], *SecurityLab*, Мн.: SecurityLab, 2004, [Online]. Режим доступа: http://www.ixbt.com/cm/informationsystem-risks012004.shtml. [просмотрено 18 декабря 2011].

97. А. Алексеев «Управление рисками. Метод CRAMM», IT Expert, М.: *ЗАО «ИТ Эксперт»*, 2010. [Online]. Режим доступа: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. [просмотрено 19 декабря 2010].

98. О. Потій, А. Лєншин, «Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу», *Збірник наукових праць Харківського університету Повітряних Сил*, № 2(24), С. 85–91, 2010.

99. А. Частиков, И. Леднева, «Использование байесовской сети при разработке экспертных систем с нечеткими знаниями», [Электронный ресурс], *Краснодар Кубанский государственный технологический университет*, 2005, [Online]. Режим доступа: http://ito.su/2000/II/5/5152.html.

100. Jeevan Jaising, Jackie Rees Krannert, «Value at Risk: A methodology for Information Security Risk Assessment», *Proceedings of The 6th INFORMS Conference on Information Systems and Technology* (CIST-2001), Miami Beach, Florida, November 2001, p. 15.

101. «Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA» [Electronic resource], *Security Risk Analysis & Assessment, and ISO 27000 Compliance*, Macclesfield: The Leading Security Risk, 2010, [Online]. Access mode: http://www.riskworld.net/.

102. Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen, «Model-Driven Risk Analysis. Chapter: A Guided Tour of the CORAS Method», 2011, *SINTEF ICT*, Oslo, Norway, pp 23-43.

103. «Information technology. Security techniques. Information security management systems. Requirements», *ISO/IEC 27001:2005*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2005, p. 34.

104. «Expression des Besoins et Identification des Objectifs de Sécurité EBIOS», *Méthode de gestion des risques*, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

105. C. Harpes, A. Adelsbach, S. Zatti, N. Peccia, «Quantitative Risk Assessment with ISAMM on ESA's Operations Data System», *Itrust consulting, 2007*. [Online]. Available: https://www.itrust.lu/ wp-content/uploads/ 2007/ 09/publications_ TTC_ 2007_abstract_risk_assessment_with_ISAMM.pdf. [Accessed: 19- Jan- 2017].

106. «IRAM2 Managing information risk is a business essential», *Information Security Forum Limited*, 2017. [Online]. Available: https://www.securityforum.org/ upl-oads/2015/03/ISF-IRAM2-ES.pdf. [Accessed: 20- Jan- 2017].

107. «Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models», *COBIT 4.1*., Rolling Meadows: IT Governance Institute, 2007, p. 196.

108. В. Олифер, Н. Олифер, *Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов*, [3-е изд.], СПб: Питер, 2006, с. 958.

109. С. Нестеров, *Анализ и управление рисками в информационных системах на базе операционных систем Microsoft, [Учебный курс.]*, Санкт-Петербург: Издательство «INTUIT», 2009, с. 136.

110. «Practical Threat Analysis in-depth», *PTA Technologies*, 2013. [Online]. Available: http://www.ptatechnologies.com/default.htm. [Accessed: 20- Jan- 2017].

111. Д. Костров, «Анализ рисков и управление ими», *Byte Россия*, №10 (62), С. 15–20, 2003.

112. С. Симонов, «Анализ рисков в информационных системах. Практические аспекты. Защита информации», *Конфидент. Безопасность компьютерных систем*, №2, С. 48-53, 2001.

113. «Compliant Information Security Risk Assessment Tool: vsRisk», [Electronic resource], IT Governance Ltd., Boise : IT Governance Ltd, 2011. [Online]. Access mode: http://www.27001.com/products/31.

114. C. Alberts, S. Behrens, R. Pethia, W. Wilson, *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM)*, Hanscom : SEI Joint Program Office, 1999, p. 72.

115. «Information technology. Security techniques. Code of practice for information security management. International standard», *ISO/IEC 17799:2005*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2005, p. 115.

116. «Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799)» [Электронный ресурс], *Callio Technologies*, М.: Представительство Callio Technologies, 2012, [Online]. Режим доступа: http://businesssoft.ru. – Загл. с экрана [просмотрено 18 марта 2011].

117. «Consultative Committee for Space Data Systems. Guide for secure system interconnection informational report», *CCSDS 350.4-G-1*, Washington: Green book November, 2007, p. 51.

118. А. Лукашов, «Монте-Карло для аналитиков. Как грамотно моделировать и измерять риски», *Риск-менеджмент*, №3, С. 73–77, 2007.

119. «Inventory of risk assessment and risk management methods», [Reference document], Paris: *Securing Europe's Information Society Regulation*, 2004, p. 460.

120. «A Guide to risk assessment and safeguard selection for Information Technology Systems», *MG-3 K1G 3Z4*, Ontario: Government of Canada, Communications Security Establishment (CSE) P.O., 1996, p. 65.

121. T. Peltier, *Information security risk analysis, London, Auerbach Publications*, 2001, p. 281.

122. W. Rowe, *An anatomy of risk*, NY: John Wiley, 1997, p. 488.

123. Anderson, Alison Shain, Michael Shain, «Anderson Risk Management», *Information Security Handbook*, New York: Stockton Press, P. 75–127, 1991.

124. «MEHARI – Overview», *Club de la Securit ´ e de l'Information Franc¸ais*, Paris: CLUSIF, 2010, p. 50.

125. «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. Book I», *The Method*, [version 2],

Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006, p. 140.

126. М. Гарсия, *Проектирование и оценка систем физической защиты*, М., Мир, 2002, с. 386.

127. «CMS Information Security Risk Assessment (RA) Methodology», *[CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)]* Baltimore : Centers for Medicare & Medicaid Services, 2002, p. 21.

128. Е. Скулыш, А. Корченко, Ю. Горбенко, С. Казмирчук, «Средства анализа и оценки риска информационной безопасности», *Інформаційна безпека. Людина, суспільство, держава*, №3 (7), С. 31-48, 2011.

129. С. Казмирчук, А. Охрименко, «Анализ и оценка риска потер государственных информационных ресурсов», *Інтегровані інтелектуальні робототехнічні комплекси (IIRTC 2012)* = Integrated Intellectual Robotechnical Complexes (IIRTC 2012), П'ята міжнар. наук.-практ. конф. : тези доп., К.: НАУ, 2012, С. 325–326.

130. А. Малюк, А. Царегородцев, Е. Макаренко, «Один из подходов к оценке рисков информационной безопасности в облачных средах», *Безопасность информационных технологий*, №4, С. 68-74, 2014.

131. А. Урзов, С. Варлатая, «Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности», *Доклады ТУСУРа*, №2 (28), С. 142-146, 2013.

132. А. Федорченко, А. Чечулин, И. Котенко, «Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей», *Информационно-управляющие системы*, №5 (72), С. 72-79, 2014.

133. А. Федорченко, А. Чечулин, И. Котенко, «Построение интегрированной базы уязвимостей», *Известия высших учебных заведений. Приборостроение*, Т.57, №11, С. 62-67, 2014.

134. В. Харченко, Алаа Мохаммед Абдул-Хади, Ю. Поночовный, «Формирование подмножеств уязвимостей доступности коммерческих Веб-сервисов», *Системи обробки інформації*, випуск 7 (114), С. 112-115, 2013.

135. А. Белобородов, А. Горбенко, «Применение баз данных уязвимостей в задачах исследования безопасности программных средств», *Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка*, Вип. 165, С. 83-85, 2015.

136. «National Vulnerability Database» [Electronic resource], *National Institute of Standards and Technology*, Gaithersburg, 2016, [Online]. Access mode: https://nvd.nist.gov/home.cfm.

137. «Банк данных угроз безопасности информации» [Электронный ресурс], *Федеральной службой по техническому и экспортному контролю России*, Москва, 2016, [Online]. Режим доступа: http://bdu.fstec.ru/.

138. «Open Sourced Vulnerability Database» [Electronic resource], *Open Security Foundation*, Lafayette, 2016, [Online]. Access mode: https:// http://osvdb.org/

139. «IBM X-Force Exchange» [Electronic resource], *IBM Corporation*, New York, 2016, [Online]. Access mode: https:// exchange. xforce. ibmcloud.com/ vulnerabilities/109429.

140. «Vulnerability Notes Database» [Electronic resource], *United States Computer Emer*gency Readiness Team, Murray Lane, 2016, [Online]. Access mode: https://www.kb.cert.org/vuls/#

141. «Vulnerabilities» [Electronic resource], *SecurityFocus, Mountain View*, 2016 [Online]. Access mode: http://www.securityfocus.com/-53r4 – Falls Church: Natl. Inst. Stand. Technol, 2013, p. 462.

142. «A Complete Guide to the Common Vulnerability Scoring System. Version 2.0», [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/v2/guide.

143. «Common Vulnerability Scoring System v3.0: User Guide» [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/user-guide.

144. «Компания Positive Technologies: Оценка уязвимостей CVSS 3.0», [Электронный ресурс], *HABRAHABR Сообщество IT-специалистов*, Москва, 2016, [Online]. Режим доступа: https://habrahabr.ru/ company/ pt/blog / 266485/.

145. «CWE™ International in scope and free for public use», [Electronic resource], MITRE, Bedford, 2016, [Online]. Access mode: http://cwe.mitre.org/index.html.

146. «X-Force – команда исследователей и разработчиков IBM Internet Security Systems (ISS)», [Электронный ресурс], *IBM Corporation*, New York, 2016, [Online]. Режим доступа: https://www.ibm.com/ru/services/iss/research.html

Глава 2. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Анализ рисков информационной безопасности

Системные аспекты защиты информации

Современная информационная отрасль – один из ведущих секторов мировой экономики, который поражает своими темпами развития. Интеграция телекоммуникационных технологий с технологиями компьютерной обработки данных стимулировала создание мирового информационного пространства и появление цивилизационной общности нового вида – информационного общества. Очевидно, что кроме традиционных природных ресурсов, неотъемлемым условием успешного существования и развития этого общества является наличие значительных и к тому же постоянно растущих информационных ресурсов, что в свою очередь обусловливает необходимость защиты этих ресурсов. Комплексным решением возникшей проблемы является построение систем защиты информации.

Следует отметить, что впервые приведенная выше проблема обозначились в конце 60-х – в начале 70-х годов двадцатого века, а особую актуальность приобрела с начала 90-х годов из-за массового внедрения в различных сферах деятельности современных информационных технологий.

С тех пор техника и методология защиты информации прошли долгий путь развития от отдельных разрозненных несложных механизмов защиты к системной концепции защиты, воплощением которой является целенаправленное использование комплекса организационно-правовых, инженерно-технических, криптографических и оперативно-розыскных мероприятий защиты информации [1, 2]. Суть системной концепции – сочетание в наиболее рациональной форме всех приведенных выше мероприятий в специальной организационно-управленческой структуре – СЗИ. Очевидно, что реализация системной концепции опирается на возможность контроля того, насколько удачным будет это сочетание, и какой уровень успешности функционирования СЗИ им будет обеспечиваться. Ответ на поставленные вопросы становится возможным

после введения системы определенных формальных критериев качества (уровня) защиты, который реализует СЗИ, причем наиболее приемлемой, универсальной и удобной формой этого критерия является количественная, так как она очень упрощает анализ и сравнение различных вариантов защиты, а в определенной ситуации позволяет оптимизировать выбор наилучшего варианта.

Построение СЗИ в общем случае представляет последовательное решение трех задач: анализа, синтеза и управления.

Содержание задачи анализа – объективная оценка угроз информации и возможного ущерба от их реализации, задачи синтеза – определение и использование наиболее эффективных механизмов защиты от угроз, которые признаны значимыми. Задача управления – обеспечение эффективной защиты информации во времени и пространстве на всех этапах ее обработки и существования в условиях изменений, происходящих в окружающей информационной, технической, технологической и социальной среде.

Воплощение системной концепции защиты информации на практике сталкивается с рядом трудностей, главными из которых являются потребность общепризнанной единой базовой методологии согласованного решении задач анализа, синтеза и управления, которая бы обеспечила применение для всех этих задач единой системы критериев (показателей), подчиненных общей цели – достижению нужного уровня защиты информации. Здесь опять возникает проблема введения уже указанных выше формализованных критериев качества СЗИ, универсальный характер которых должен обеспечить проработку, сопоставление, анализ различных вариантов СЗИ и оптимизацию выбора лучшего в условиях требуемого (заданного) уровня защиты.

Анализ публикаций по вопросам защиты информации, материалов научно-исследовательских работ и практических разработок СЗИ, изучение содержания международных, региональных, национальных, отраслевых нормативных документов и стандартов [3-9] позволяет утверждать, что в качестве подобной системной методологии может быть использован подход, известный как оценивание и управления информационными рисками (менеджмент информационных рисков) [7-14]. Опираясь на данный подход, следует определить, что входит в состав информации, требующей защиты,

оценить необходимую степень ее защиты, выбрать стратегию будущего развития информационной структуры организации-владельца информации и поддерживать на должном уровне безопасность этой информации.

Суть применения методологии оценивания рисков для построения СЗИ заключается в сопоставлении исходного и остаточного информационных рисков (рисков до и после построения СЗИ), которые рассчитываются из оценки возможных убытков, возникающих вследствие возможной реализации информационных угроз до или после внедрение СЗИ. По результатам сопоставления делается вывод о целесообразности использования тех или иных механизмов защиты информации, их эффективности и эффективности функционирования СЗИ в целом.

В формальном представлении имеем:

$$R_i = P_i Q_i,$$

$$r_i = p_i P_i Q_i,$$

где P_i – вероятность реализации *i*-ого информационного риска, Q_i – потери (в денежных единицах или баллах), обусловленные реализацией *i*-той угрозы, p_i – вероятность реализации *i*-той угрозы после внедрения СЗИ из-за наличия уязвимости в системе защиты по этой угрозе.

Имея риски R_i, r_i, можно оценить эффективность защиты от *i*-той угрозы:

$$E_i = (R_i - r_i) / R_i = 1 - p_i,$$

где показатель E_i может изменяться от 1 (случай «абсолютной защищенности» от *i*-той угрозы, r_i = 0) до 0 (нулевую эффективность защиты имеем в случае $R_i = r_i$, то есть при абсолютной, стопроцентной уязвимости СЗИ по *i*-той угрозе). Другая форма функционала эффективности защиты задается выражением:

$$e_i = R_i / r_i = 1 / p_i. \qquad (2.1)$$

Диапазон изменений e_i – от 1 (абсолютная неэффективность) до бесконечности ∞ (абсолютно эффективная защита).

Еще один показатель эффективности защиты, учитывающий затраты на реализацию собственно механизма защиты, может задаваться соотношением [2]:

$$W_i = (R_i - r_i) / q_i = (1 - p_i) P_i Q_i / q_i, \qquad (2.2)$$

где q_i – оценка стоимости затрат на создание и внедрение механизма (механизмов) защиты против *i*-той угрозы.

Приведенные выше выражения позволяют оценить эффективность фрагментарной защиты от отдельной частной угрозы. Однако защищаемая информация может подвергаться воздействию ряда потенциальных угроз, поэтому кроме анализа частных рисков R_i, принципиальным является определение совокупной вероятности P реализации существующей для информации опасности (в любой форме представления) и совокупного (интегрального) риска R. Если информация, подлежащая защите, состоит из нескольких отдельных информационных ресурсов IP_1,..., IP_m, то объединение рисков по всем m составляющими и расчет соответствующего объединенного остаточного риска позволяет оценить эффективность СЗИ по всей совокупности информационных ресурсов. Определив общесистемный риск идентификаторами $R_\Sigma = r_\Sigma$, можно рассчитать по уже применяемыми ранее формулам (2.1), (2.2) показатели $E_{\Sigma 1}, E_{\Sigma 2}$, непосредственно характеризующих эффективность СЗИ.

В практике защиты популярны системные показатели эффективности СЗИ типа [15]

$$RIO = (R_\Sigma - r_\Sigma - q_\Sigma) / q_\Sigma$$

– показатель возврата инвестиций (*ROI* – return on investment), q_Σ – общие затраты на создание и обслуживание СЗИ, так называемая совокупная стоимость владения (*TCO* – total cost of ownership), или

$$W_\Sigma = (R_\Sigma - r_\Sigma) / Q,$$

где знаменатель Q может быть разным по содержанию. Это, в частности, общая стоимость определенного ОИД, где циркулирует ИсОД, стоимость ИсОД и информационных услуг по ее обработке, общая стоимость информационных ресурсов, которые задействованы в информационно-аналитической системе, которую защищает СЗИ и тому подобное.

Системные показатели такие, как W_{Σ}, позволяют сопоставить затраты на создание СЗИ на объекте информационной деятельности (ОИД), которая обеспечивает определенные требования к уровню защиты информации с ограниченным доступом (ИсОД), с общеэкономическими характеристиками ОИД или показателям информационной деятельности, например, со скоростью передачи информации в защищенной системе связи (в защищенной системе связи скорость передачи информации существенно зависит от сложности алгоритма криптозащиты, которая в свою очередь напрямую связана с требованиями к необходимому уровню защиты информации в канале связи).

Угрозы информации. Классификация угроз информации в ИТС

Действия, которые приводят к реализации потенциальных опасностей, ведущих к снижению ценности информационных ресурсов, называются неблагоприятными. Потенциально возможное неблагоприятное влияние называется угрозой.

Угроза информации (информационная угроза) – любые обстоятельства или события, которые могут быть причиной нарушения политики безопасности информации и / или нанесения ущерба ИТС.

Поскольку, с точки зрения защищенности информации принято выделять три ее **критических свойства: конфиденциальность, целостность и доступность**, то угрозы, реализация которых приводит к потере информации любого из названных свойств, соответственно называются **угрозами конфиденциальности, целостности или доступности** информации, а риски, возникающие в результате реализации этих угроз – **информационными рисками**.

Результаты реализации угрозы могут влиять на информацию как непосредственно, так и косвенно. Например, потеря управляемости ИТС в результате реализации каких-либо деструктивных действий может привести к неспособности СЗИ ИТС обеспечивать защиту информации и, как результат, к потере определенных свойств передаваемой/обрабатываемой информации. **Попытка реализации информационной угрозы называется атакой**.

Этап анализа возможных угроз информации в ИТС необходим для фиксации на определенный момент времени состояния ИТС (конфигурации аппаратных и программных средств, реализованной технологии обработки информации), в частности, определения возможных неблагоприятных воздействий на каждый компонент системы и обрабатываемую с его помощью информацию. Обеспечить защиту информации от всех возможных неблагоприятных воздействий на нее невозможно, хотя бы потому, что невозможно полностью установить перечень угроз и способов их реализации, поэтому нужно выбрать из всех возможных неблагоприятных воздействий только те, которые могут реально произойти и нанести вред информационным активам.

Угрозы обрабатываемой в ИТС информации зависят от характеристик внутренней системы, физической среды, персонала и обрабатываемой информации. Угрозы могут иметь или объективную природу, например: изменение условий физической среды (пожары, наводнения и т.п.), отказ элементов системы, или субъективную, в частности, ошибки персонала или действия злоумышленника.

Угрозы, имеющие субъективную природу, могут быть случайными или преднамеренными.

Идентификация угроз (определение множества угроз, реализация которых возможна в конкретной ИТС) предусматривает рассмотрение источников угроз и последствий, обусловленных реализацией угроз, а также их классификацию.

Все источники угроз информации, обрабатываемой в конкретной ИТС, можно разделить на три основные группы:

− антропогенные угрозы, обусловленные действиями субъекта (злоумышленника);

− техногенные угрозы, обусловленные особенностями и условиями функционирования технических средств в ИТС;

− угрозы, обусловленные стихийными (природными) источниками опасности.

Первая группа широка и составляет очевидный интерес с точки зрения организации защиты от угроз данного типа, так как действия субъекта можно попытаться предсказать, оценить и принять

адекватные меры. Методы и меры противодействия этим угрозам (контрмеры) непосредственно зависят от разработчиков СЗИ.

Субъекты, действия которых направлены на нарушение защищенности информации, могут быть как внешние: криминальные структуры, недобропорядочные партнеры, конкуренты, политические противники, так и внутренние – персонал ИС, работники организации.

По данным международного и отечественного опыта, действия злоумышленника способны привести к ряду нежелательных последствий, среди которых можно выделить следующие:

− кража технических средств ИТС, носителей информации, информации, средств доступа к информации;

− подмена (модификация) операционных систем, систем управления базами данных, прикладных программ, информации (данных), отрицание фактов отправки сообщений, паролей и атрибутов доступа

− уничтожение (разрушение) технических средств ИТС, носителей информации, программного обеспечения, информации, паролей и ключевой информации;

− нарушение нормальной работы ИТС: снижение скорости обработки информации, снижения пропускной способности каналов связи, уменьшение объемов свободной оперативной памяти, уменьшение объемов свободного дискового пространства, нарушения электропитания технических средств;

− ошибки при инсталляции ПО, ОС, СУБД, при написании прикладного ПО, при эксплуатации ПО, при эксплуатации технических средств;

− перехват информации через побочное электромагнитное излучение технических средств ИТС, за счет наводок по линиям электропитания и наводок по посторонним проводникам, по акустическому каналу, от средств связи при подключении к каналам передачи информации, за счет нарушения установленных правил доступа (взлом).

Вторая группа содержит угрозы, которые непосредственно зависят от свойств техники и поэтому требуют постоянного внимания. Технические средства, содержащие каналы реализации потенциальных угроз защищенности информации, могут быть как внутрен-

ними (некачественные технические средства обработки информации, некачественные программные средства обработки информации, вспомогательные средства (охрана, сигнализация, телефония), другие технические средства, применяемые в организации), так и внешними: средства связи, близко расположенные опасные производства, сети инженерных коммуникаций (энерго-, водоснабжения, канализации), транспорт.

Последствиями применения таких технических средств, которые непосредственно влияют на защищенность информации, могут быть:

1. Нарушение нормальной работы технических средств ИТС:
- нарушение работоспособности средств обработки информации;
- нарушение работоспособности каналов передачи данных;
- старение носителей информации и средств ее обработки;
- нарушение установленных правил доступа;
- электромагнитное воздействие на технические средства.

2. Уничтожение (разрушение) информационных активов ИТС:
- программного обеспечения, ОС, СУБД;
- средств обработки информации;
- помещений;
- информации;
- персонала.

3. Модификация (изменение) информационных активов ИТС:
- программного обеспечения, ОС, СУБД;
- информации при передаче по каналам передачи данных.

Третью группу составляют угрозы, которые плохо поддаются прогнозированию и поэтому меры для их предотвращения должны применяться, по возможности, всегда, но не обязательно к ИТС как к объекту защиты, а шире, ко всем элементам технической инфраструктуры предприятия или организации. Стихийные источники опасностей содержат потенциальные угрозы защищенности информации, которые, как правило, являются внешними по отношению к данному объекту, под ними понимаются, прежде всего, природные катаклизмы: пожары, землетрясения, наводнения, ураганы, различные необъяснимые явления, другие форс-мажорные и непредвиденные обстоятельства.

Эти природные и необъяснимые явления опасны для всех элементов ИТС и могут привести к таким последствиям, как уничтожение (разрушение) технических средств обработки информации, носителей информации, программного обеспечения, информационных ресурсов (файлов данных), информации в средствах обработки и при ее передаче по телекоммуникационным каналам, разрушению помещений и сооружений, где располагаются объекты ИТС, созданию угроз здоровью и жизни персонала.

С учетом указанных источников воздействий, последствий и целей реализации угроз можно выделить следующие основные классификационные признаки угроз информации, обрабатываемой в ИТС:

− свойства информации, к нарушению которых может привести угроза (нарушение конфиденциальности, целостности или доступности информации);

− область поражения и последствия реализации угроз для ИТС, ее подсистем и элементов, различных форм и видов информационного обеспечения, субъектов и объектов ИТС, пользователей, активов, зависящих от качества функционирования ИТС;

− интенсивность (силу) факторов поражения (разрушительные, дестабилизирующие, катастрофические и т.п.);

− принадлежность угрозы к внешнему окружению ИТС или к ее внутрисистемной среды;

− форму и степень социальной опасности (коллизия, конфликт, проступок, преступление, авария, катастрофа).

Результат проведения анализа рисков формирует основы для определения необходимых мер защиты. Сам процесс анализа включает в себя нахождение ответа на ряд главных вопросов: какие именно информационные активы нуждаются в защите, какие угрозы могут возникнуть в системе, вероятность реализации этих угроз и какой ущерб они могут нанести. Оценивание риска состоит в последовательном прохождении следующих этапов: определения степени детализации и методологии анализа и оценивания риска, оценивания ценности активов, идентификации и определения вероятности угроз, измерения уровня риска.

Международные стандарты управления и безопасности информационных технологий

Проблема оценивания и исследования информационных рисков обычно ассоциируется с британским стандартом BS 7799, в первую очередь с его двумя частями: первой – BS 7799-1 «Правила менеджмента безопасности информации» и второй – BS 7799-2 «Системы менеджмента безопасности информации», в которых впервые вопросы анализа состояния безопасности информации и формирования ее защиты были непосредственно связаны с информационными рисками [7, 11]. Собственно, аспекты оценки и управления рисками, гармонизированные с содержанием двух первых частей, были детально рассмотрены в третьей части стандарта BS 7799-3 «Руководство по менеджменту рисками безопасности информации» [5]. Однако первым международным стандартом менеджмента рисками стал стандарт ISO / IEC TR 13335-3 «Руководство по менеджменту безопасности информационных технологий» (1998 г.), который, как и другие стандарты серии ISO / IEC 13335, является национальным стандартом Украины. Через десять лет, в 2008 г. был издан стандарт ISO / IEC 27005: 2008 – Information technology – Security techniques – Information security risk management (Информационные технологии – Технологии безопасности – Менеджмент рисками безопасности информации) [9], который сейчас является одним из ведущих нормативных документов в сфере управления информационными рисками.

Практически все современные стандарты в области безопасности отражают общий подход к организации управления рисками, сложившийся в международной практике. При этом управление рисками представляется как базовая часть системы менеджмента качества организации. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по информационной безопасности реализовывать любые методы, средства и технологии оценивания, обработки и управления рисками.

Считается, что международные стандарты, учитывая, что они созданы на основе анализа и обобщения лучших методов, апробированных, как большими группами профессионалов, так и ведущими организациями на практике, в большинстве случаев определяют

лучшие варианты действий при возникновении инцидентов в информационной безопасности. Использование стандартов увеличивает ценность создаваемой информационной системы или технологии, но, к сожалению, нет таких стандартов, которые бы охватили все аспекты управления, безопасности и качества.

Эволюцию развития стандартов в области менеджмента рисками безопасности информации можно представить схемой, изображенной на рис. 2.1 [16].

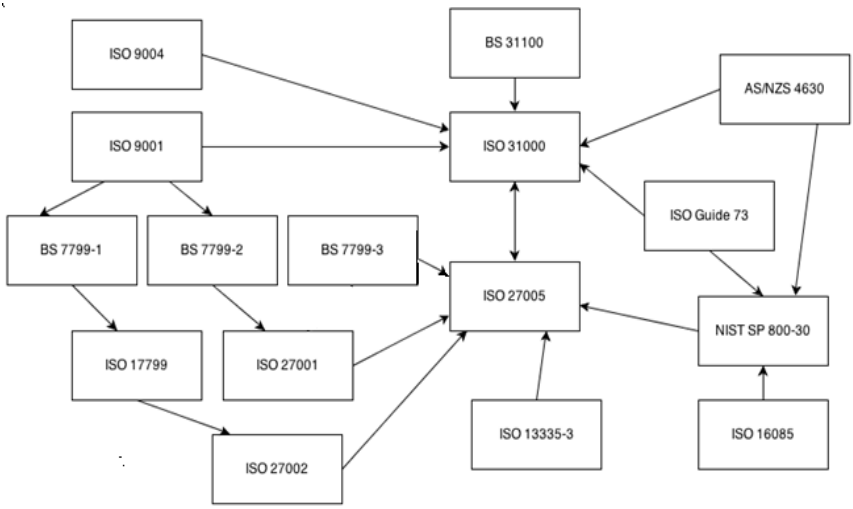


Рис. 2.1. Эволюция стандартов менеджмента рисками безопасности информации

Очевидно, что смысл эволюции – выход нового стандарта на более высокий качественный уровень через «восприятие опыта» от стандартов – предшественников и обобщения опыта и результатов применения стандартов из смежных отраслей. На сегодняшний день можно констатироваться, что состоялся позитивный процесс замещения старой серии стандартов информационной безопасности ISO / IEC TR 13335, новой серией стандартов в области управления информационной безопасностью – ISO / IEC 27000. Новый стандарт ISO / IEC 27005 заменил сразу два морально устаревших стандартов ISO / IEC TR 13335-3 [17] и ISO / IEC TR 13335-4 [18],

которые, однако, остались в числе базовых документов нового стандарта. Кроме того, стандарт ISO / IEC 27005 также опирается на нормативно – методические документы, приведенные в его библиографическом перечне: ISO / IEC 16085 [6], BS 31100 [19], AS / NZS 4360 [3] и NIST SP 800-30 [10]. Существенное влияние на содержание нового стандарта имела разработка стандарта ISO 31000: 2009 – Risk management – Principles and guidelines (Управление рисками. Принципы и рекомендации), которая длилась практически одновременно с разработкой ISO / IEC 27005.

Стандарт ISO / IEC 31000 обобщил в себе лучшие тенденции мировой практики по управлении рисками. В библиографическом списке этого стандарта такие стандарты, как: ISO / IEC 9001 – общие требования к системам менеджмента качества, ISO / IEC 9004 – рекомендации для устойчивого достижения целей в системах управления качеством, BS31100 – набор практических и конкретных рекомендаций для менеджера информационной безопасности, ISO / IEC Guide 73 – набор терминов для управления рисками, уже упомянутый выше AS / NZS 4360 – общие требования к условиям управления рисками. Вся нормативная документация, на которой базируется стандарт ISO / IEC 31000, относится к области управления и контроля качеством и применима к различным сферам деятельности, включая и сферу информационной безопасности.

Обобщение лучшего межотраслевого опыта является одним из преимуществ стандарта ISO / IEC 27005, в этом смысле сложилась такая ситуация: с одной стороны – сильная теоретическая база с практикой управления безопасностью информации, а с другой – лучшее из опыта управления и контроля качества систем менеджмента, проверенное во многих сферах применения.

Следует отметить, что вопреки распространенным ожиданиям, новый стандарт ISO / IEC 27005 вовсе не является международной версией стандарта BS 7799-3 [5]. Более того, в нем даже не встречается упоминания о последнем стандарте. Структура и содержание этих стандартов существенно различаются, существенно разные и источники разработки. Неизменным остается лишь общий понятийный аппарат, общий подход к процессу управления рисками.

В общем можно сделать вывод о том, что в разработке стандарта ISO / IEC 27005, в отличие от предыдущих стандартов серии ISO / IEC 27000, в которых использовались исключительно наработки BSI и других британских организаций, в полной мере учтен существующий международный опыт.

Методики и рекомендации приведенных выше стандартов базируются на двух основных подходах к представлению оценок информационных рисков: качественном и количественном.

Задачей качественной оценки является определение возможных видов рисков, оценка принципиального уровня серьезности угроз, а также выделение факторов, влияющих на уровень обоснования различных возможных контрмер. Эти методики не дают количественные или денежные значения рискам или их компонентам. Они довольно популярны, относительно простые и разработаны, как правило, на основе требований международного стандарта ISO / IEC 17799: 2005 [7].

Количественные методики на выходе предоставляют реальные и осмысленные количественные значения всех показателей и элементов процесса анализа рисков. Этими элементами могут быть стоимость защитных мероприятий, ценность актива, ущерб для бизнеса, частота возникновения угрозы, эффективность защитных мероприятий, вероятность использования уязвимости и так далее. Количественный анализ позволяет получить конкретное значение вероятности реализации угрозы. Каждый элемент в процессе анализа вводится в количественном виде в выражения для определения общего и остаточного риска.

Также довольно часто используется комбинация этих двух подходов: как правило, на начальных этапах анализа информационных рисков используется качественный подход, а на заключительном, то есть именно при получении оценки – количественный.

Учитывая, что оценивание рисков на качественном уровне не позволяет однозначно сравнить затраты на мероприятия по обеспечению защиты информации и полученную от них отдачу (в виде снижения интегрального риска), сосредоточимся на более точном количественном подходе. Отметим, что в этом случае процедура построения СЗИ на базе методологии информационных рисков при

применении положений основных стандартов характеризуется рядом «узких» мест.

Во-первых, это необходимость параметризации рисков. Распространенное математическое выражение, на основе которого вычисляют риск, обусловленный возможной реализацией угрозы *T*, имеет вид:

$$r_T = P_T q = P_t P_V q ,$$

где P_T – вероятность реализации угрозы *T*, q – убытки, которые возникают в условиях реализации угрозы *T*, P_t – вероятность возникновения (активации) угрозы *T*, P_V – вероятность удачного использования злоумышленником уязвимостей информационной системы, что приводит к реализации угрозы *T*. То есть расчет риска требует знания двух (P_T, q) или трех (P_t, P_V, q) параметров риска, которые обычно определяются экспертным путем [13, 14], что может существенно ухудшить качество оценок рисков, а в худшем случае – абсолютно непредсказуемо повлиять на конечные результаты менеджмента рисков.

Во-вторых, наличие нескольких угроз (уязвимостей) характеризуется соответствующими частными рисками, совокупное влияние которых описывается интегральным риском, определение которого в общем случае может быть достаточно сложным [20].

В-третьих, методики управления рисками, разработанные в соответствии с положениями стандартов, чаще всего опираются на переборный подход: рассматривается несколько возможных вариантов построения СЗИ, в которых уровни рисков (интегрального риска) уменьшаются до приемлемых значений, и дальше по решению эксперта определяется рабочий вариант (возможно, он выбирается как наименее дорогой).

При этом вопрос качества рабочего варианта СЗИ (оптимальности принятого решения о выборе этого варианта СЗИ), эффективности инноваций в построение СЗИ организации практически не исследуются.

Замена эксперта любым инструментально – программным средством (ИПС) принципиально ситуации не меняет, потому что прототипом при разработке этих ИПС выступает именно эксперт, в связи с чем практически все наиболее распространенные ИПС – это

интеллектуализированные информационные системы (системы поддержки принятия решений, экспертные системы и т.д.), в которых реализованы те или другие методы отображения и обработки знаний.

Определенной альтернативой управлению рисками на базе представленных в стандартах методик является применение в менеджменте рисков математических моделей, связывающих уровень рисков (убытков), обусловленных реализацией информационных угроз, с объемом вложений в СЗИ [21, 22].

Применение этих моделей для анализа и исследования рисков имеет целью среди прочего обеспечить возможность оценки эффективности вложений в СЗИ и прогнозирования характеристик рисков в зависимости от уровня инвестиций в систему защиты.

Общее описание процесса менеджмента рисков информационной безопасности

Рассмотрим подробнее актуальный на сегодняшний день международный стандарт ISO / IEC 27005: 2008 – Information technology – Security techniques – Information security risk management (Информационные технологии – Технологии безопасности – Менеджмент рисков безопасности информации). Данный стандарт предоставляет руководство по менеджменту рисками безопасности информации в организации, в частности систематизирует требования к системе менеджмента защиты информации (СМЗИ), и предназначен для руководителей и персонала, занимающихся в организации вопросами менеджмента риска безопасности информации, и, при необходимости, для других подразделений, сторон, лиц, имеющих отношение к этому виду деятельности.

Систематизированный подход к менеджменту рисков информационной безопасности необходим для того, чтобы идентифицировать потребности организации, касающиеся требований информационной безопасности и создать эффективную СМЗИ. Этот подход должен быть применим к среде организации и, в частности, должен поддерживать менеджмент рисков для всей организации, обеспечивая эффективное и своевременное рассмотрение рисков там и тогда, где и когда это необходимо. Менеджмент рисков информационной безопасности должен быть неотъемлемой частью всех

видов деятельности, связанных с менеджментом информационной безопасности, а также должен применяться для реализации и поддержки функционирования всей системы менеджмента рисков организации.

Менеджмент рисков безопасности информации должно быть непрерывным процессом. Данный процесс должен устанавливать контекст, поддерживать оценку и обработку рисков, обеспечивать использование плана обработки риска для реализации, способствовать выработке рекомендаций и решений. Менеджмент риска связан с анализом того, что может произойти и какими могут быть возможные последствия, прежде чем выработать решение о том, что и когда должно быть сделано для снижения риска до приемлемого уровня.

Менеджмент рисков безопасности информации должен способствовать следующему:

− идентификации рисков;

− оценке рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;

− изучение вероятности и потенциальных последствий этих рисков;

− установление порядка приоритетов в рамках обработки рисков;

− установление приоритетов мероприятий по снижению имеющих место рисков;

− привлечению заинтересованных сторон к принятию решений о менеджменте рисков и поддержание их осведомленности о состоянии менеджмента риска;

− эффективности мониторинга обработки рисков;

− проведению регулярного мониторинга и просмотра процесса менеджмента рисков;

− сбору информации для совершенствования подхода к менеджменту рисков;

− подготовке менеджеров и персонала в сфере управления рисками.

Процесс менеджмента рисков информационной безопасности может быть применен ко всей организации, к ее любой отдельной части (например, подразделению, месту физического пребывания,

сервису), к любой информационной системе, существующим, планируемым или имеющимся аспектам управления (например, к планированию непрерывности бизнеса).

Процесс менеджмента рисков безопасности информации состоит из установления контекста, оценки риска, обработки риска, принятие риска, обмена информацией относительно риска, а также мониторинга и пересмотра риска. Как показано на рис. 2.2, процесс менеджмента риска безопасности информации может быть итеративным для таких видов деятельности, как оценивание риска и / или обработка риска. Итеративный подход к проведению оценивания риска может увеличить глубину и детализацию оценивания при каждой итерации. Итеративный подход дает хороший баланс между уменьшением времени и усилий, которые затрачиваются на проведение контроля рисков, в то же время обеспечивая уверенность в том, что высокоуровневые риски рассматриваются соответствующим образом.

Контекст впервые устанавливается тогда, когда проводится оценивание высокоуровневого риска. Если оно обеспечивает достаточную информацию для эффективного определения действий, необходимых для снижения риска до приемлемого уровня, задание является исполненным и далее следует обработка риска. Если информация недостаточна, то проводится другая итерация оценки риска с помощью пересмотренного контекста (например, критериев оценки рисков, критериев принятия рисков или критериев воздействия), возможно на ограниченных частях полной области проведения анализа рисков (см. рис. 2.2, точка принятия решений о риске № 1).

Эффективность обработки риска зависит от результатов оценивания риска. Возможно, что обработка риска не будет сразу же приводить к приемлемому уровню остаточного риска. В этой ситуации может потребоваться, если необходимо, другая итерация оценивания риска с измененными параметрами контекста (например, критериев оценивания риска, принятие риска или воздействия), за которой последует дополнительная обработка риска (см. рис. 2.2, точка принятия решений о риске № 2).

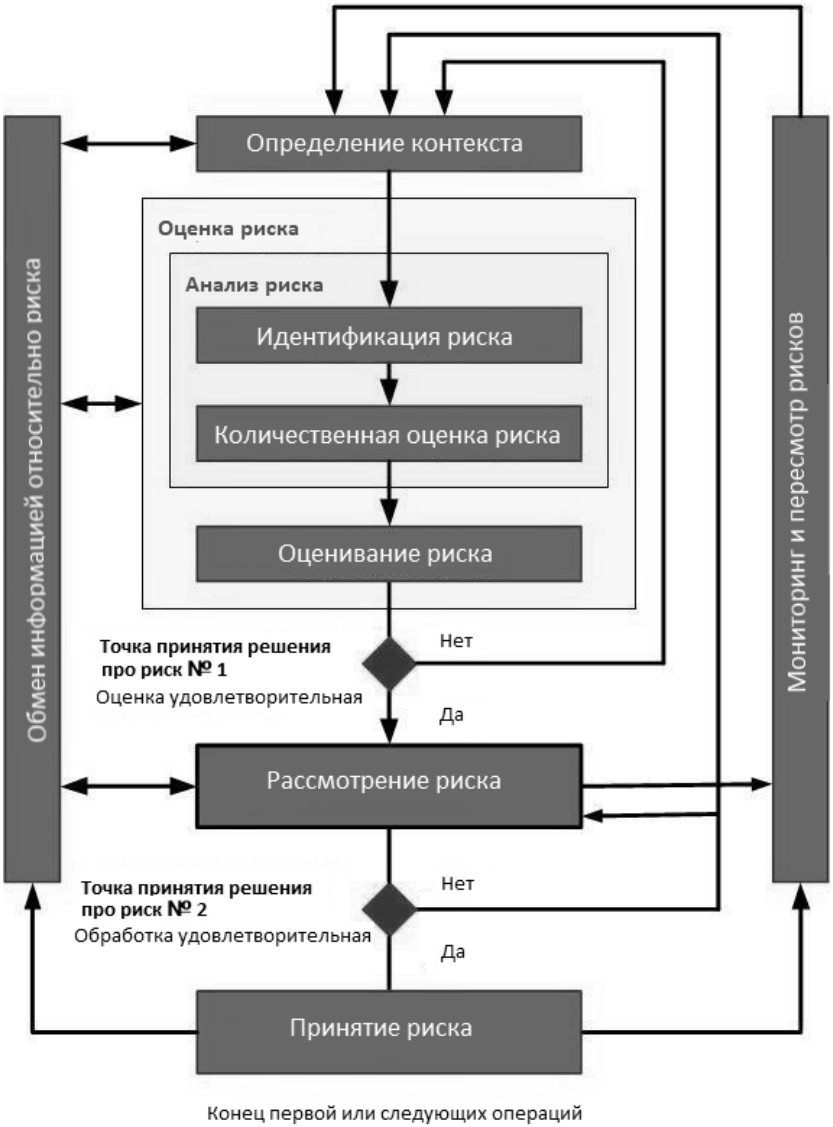


Рис. 2.2. Процесс менеджмента рисков информационной безопасности по стандарту ISO/IEC 27005

Деятельность по принятию риска должна обеспечивать уверенность в том, что остаточные риски однозначно принимаются руководством организации. Это особенно важно в ситуации, когда внедрение средств контроля рисков не осуществляется или откладывается (например, из-за стоимости).

Важно, чтобы во время всего процесса менеджмента рисков безопасности информации и обработке рисков осуществлялся обмен информацией о рисках между соответствующим руководством и операционным персоналом. Даже до обработки рисков информация об идентифицированных рисках может быть очень ценной для осуществления менеджмента инцидентов и может способствовать снижению потенциального ущерба. Осведомленность руководства и персонала о рисках, природе средств контроля, применяемых для снижения рисков, и проблемных областях организации помогает им в рассмотрении инцидентов и неожиданных событий. Детализированные результаты каждой деятельности, входящей в процесс менеджмента рисков безопасности информации, и результаты, полученные от двух точек принятия решений о рисках, должны быть задокументированы.

Следует отметить, что понимание положений стандарта ISO / IEC 27005 и эффективное применение его в практической деятельности в значительной степени базируется на основных принципах и базовых требованиях к построению и функционированию системы менеджмента безопасности информации, приведенных в стандарте ISO / IEC 27001: 2005 – Information technology – Security techniques – Information security management systems – Requirements (Информационные технологии – Технологии безопасности – Системы менеджмента безопасности информации – Требования).

Требования данного документа в определенной степени абстрактны и не привязаны к специфике любой области деятельности, они могут применяться какой-либо организацией независимо от ее типа, размеров и характера бизнеса. Системы СМЗИ базируются на процедуре оценивания и анализа рисков, направленной на расчет интегральных показателей защищенности ключевых информационных активов, и выборе мер по минимизации рисков до приемлемого остаточного уровня. В соответствии с ISO / IEC 27001, СМЗИ должна проектироваться таким образом, чтобы обес-

печить выбор адекватных и соответственных мер по обеспечению безопасности.

В основу модели организации процессов СМЗИ данного стандарта заложен классический замкнутый цикл менеджмента Plan-Do-Check-Act (PDCA, «планирование – осуществление – проверка – действие»), который известен как «цикл Деминга» (см. рис. 2.3).

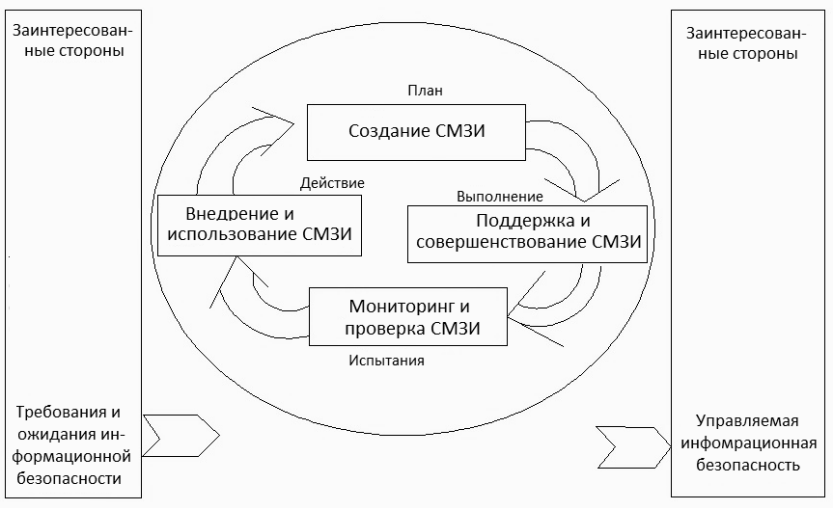


Рис. 2.3. Применение модели PDCA в процессах СМЗИ

Стандарт ISO/IEC 27001:2005 описывает:

- требования для разработки, реализации, эксплуатации, мониторинга, ревизии, поддержания и совершенствования СМЗИ;
- требования к документации и управление ею;
- обязанности руководства;
- менеджмент ресурсов, то есть обеспечение и работу с ними;
- требования к анализу СМЗИ со стороны руководства, в частности входящие / исходящие данные для анализа;
- цели управления и средства управления.

В стандарте ISO / IEC 27001 определяется, какие средства контроля, реализуемые в рамках сферы применения, границ и контекста СМЗИ, должны основываться на риске. Применение процесса менеджмента рисков безопасности информации должно удовле-

творять этому требованию. Существует много подходов, с помощью которых процесс может быть успешно внедрен в организации. В любом случае организация должна использовать подход, который наилучшим образом соответствует обстоятельствам каждого конкретного применения процесса менеджмента.

Для СМЗИ установления контекста, оценивание риска, разработка плана обработки риска и принятия риска является частью фазы «планирование». В фазе «осуществление» СМЗИ действия и средства контроля, необходимые для снижения риска до приемлемого уровня, реализуются в соответствии с планом обработки риска. В фазе «проверка» СМЗИ менеджеры определяют потребность в пересмотре обработки риска с учетом последних инцидентов и изменений контекста. В фазе «действие» осуществляются любые необходимые работы, включая повторное инициирование процесса менеджмента рисков безопасности информации.

Рассмотрим таблицу, которая содержит описания действий менеджмента рисками информационной безопасности, касающихся четырех фаз процесса СМЗИ (табл. 2.1). В таблице суммируются виды деятельности, связанной с менеджментом риска, значимые для четырех фаз процесса СМЗИ.

Таблица 2.1. Регулирование СМЗИ и процесс менеджмента рисков безопасности информации

Процесс СМЗИ	**Процесс менеджмента риска информационной безопасности**
Планирование (Plan)	Установление контекста. Оценивание риска. Разработка плана обработки риска. Принятие риска.
Осуществление (Do)	Реализация плана обработки риска
Проверка (Check)	Непрерывный мониторинг и рассмотрение рисков
Действие (Act)	Поддержка и улучшение рисков информационной безопасности. Процесс менеджмента

Первым и поэтому определяющим для последующих этапов менеджмента рисков безопасности информации является этап установки области применения и границ процесса менеджмента рисков безопасности информации. В рамках этого этапа реализуется де-

тальное изучение организации, что дает возможность воссоздать характерные элементы, которые определяют особенности организации. Это касается цели, бизнеса, назначения, ценностей и стратегий организации. Особенности организации должны быть определены рядом с элементами, которые способствуют их развитию (например, заключение контрагентных договоров).

Трудности такой деятельности заключаются в точном понимании структуры организации. Определение реальной структуры дает понимание роли и важности каждого подразделения в достижении целей организации. Ниже приведены основные содержательные разделы, последовательное выяснение сущности которых формирует процедуру изучения организации.

Основная цель организации. Основная цель организации может определяться как причина того, почему она существует (ее сфера деятельности, сегмент рынка и т.д.).

Ее бизнес. Бизнес организации, определяемый методами и накопленным опытом (ноу-хау) ее сотрудников, дает ей возможность реализовывать свое предназначение. Он является специфическим полем деятельности организации и часто определяет ее культуру труда.

Ее назначение. Организация достигает своей цели посредством реализации своего предназначения. Для определения ее назначения обеспечиваемые сервисы и изготавливаемые продукты должны быть определены в отношении конечного пользователя.

Ее ценности. Ценностями являются основные принципы или хорошо определенный кодекс поведения, применяемые для осуществления бизнеса. Это может касаться персонала, отношений с внешними агентами (клиентами, например), качества поставляемых продуктов или обеспечиваемых сервисов.

*Структура организации.*Существуют различные типы структуры:

− филиальная структура: каждое подразделение работает под руководством менеджера подразделения, ответственного за принятие стратегических, административных и операционных решений, касающихся его подразделения;

− функциональная структура: функциональное руководство осуществляется по процедурам, сущности работы и, иногда, по

функциям принятия решений или планирования (например, производство, ИТ, кадры, маркетинг и т.д.).

Замечание:

− подразделение, которое существует в пределах организации с филиальной структурой, может быть организовано как функциональная структура и наоборот;

− структура организации, имеющей элементы обоих типов структуры, называется матричной.

При любой организационной структуре могут различаться следующие уровни:

а) уровень принятия решений (определение стратегической ориентации);

б) уровень руководства (координация и менеджмент);

в) операционный уровень (виды деятельности, связанные с производством и поддержкой).

Диаграмма организации.

Структура организации представляется схематически на диаграмме организации. При таком представлении главное место должно отводиться линиям отчетности и делегирования полномочий, кроме того, также должны включаться и другие отношения, которые, даже если они не основываются на каких-либо формальных полномочиях, являются, тем не менее, линиями информационного потока.

Стратегия организации.

Содержит концептуальное изложение руководящих принципов организации. Стратегия организации определяет направление и развитие, организации, обеспечивающее устойчивость бизнеса в условиях возможных изменений внешнего и внутреннего контекста ее функционирования.

2.2. Практические аспекты оценивания рисков реализации угроз в информационных системах

Вычисление обобщенных рисков на базе сведений об атаках и угрозах

Одним из важных показателей уровня безопасности информации в ИС организации, который позволяет в совокупности учесть

влияние всего множества актуальных для данной ИС угроз, является обобщенный риск R, называемый также интегральным риском. Нахождение обобщенного риска – завершающий этап процесса АОР, в ходе которого результаты АОР, представленные профилем рисков, отражаются в скалярный показатель. Очевидно, что как структура обобщенного риска, так и процедура его вычисления должны обеспечивать объективность и корректность производимого отображения. Однако корректность именно этих аспектов оценивания рисков часто оказывается сомнительной. Рассмотрим проблемы, возникающие при применении одной из наиболее распространенных форм показателя обобщенного риска, называемой суммарным риском [20, 23, 24]:

$$R_{\Sigma} = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i q_i, \qquad (2.3)$$

где r_i – значение риска, обусловленное возможным влиянием некоторого опасного фактора v_i, вероятность реализации которого – p_i, а q_i – потери организации, которые возникают в случае реализации влияния этого фактора на объект риска, в данном случае – на ИС организации. Логику возникновения и развития негативных влияний на ИС в общем случае можно описать следующей схемой:

Опасности среды функционирования ИС ⇒ влияние опасных явлений и процессов на элементы ИС ⇒ угрозы информационным активам ИС ⇒ атаки уязвимостей ИС ⇒ потери организации, обусловленные реализацией угроз.

При этом в ходе АОР рассчитывается три вида рисков: риски атак, реализующих ту или иную угрозу, риски отдельных угроз и обобщенный риск R, обусловленный опасностями среды функционирования ИС (т.е. совместными действиями всей совокупности угроз, генерируемых средой функционирования ИС).

Если воспользоваться формулой (2.3) для расчета риска, связанного с воздействием определенной угрозы, которая может быть реализована любой успешной атакой α_j из множества A=$\{\alpha_j\}$, $j = \overline{1, k_i}$, получим такое выражение:

$$r_i = \sum_{j=1}^{k_i} \rho_j = \sum_{j=1}^{k_i} p_{aj} q_i = q_i \sum_{j=1}^{k_i} p_{aj} \,, \qquad (2.4)$$

где $\rho_j = p_{aj} q_i$ – частный риск, обусловленный успехом атаки α_j, позволяющей реализовать угрозу t_i, используя уязвимость v_j, p_{aj} – вероятность успешного завершения атаки α_j. Соотношение (2.4) выведено в предположении, что реализация угрозы с помощью любой из атак $\{\alpha_j\}$, $j = \overline{1, k_i}$, ведет к одной и той же величине потерь q_i. При этом, учитывая, что для произвольной вероятности p_{aj} справедливо неравенство $0 \le p_{aj} \le 1$, очевидно утверждение

$$0 \le \sum_{j=1}^{k_i} p_{a\,j} \le k_i \,. \qquad (2.5)$$

С другой стороны, т.к. риск, обусловленный возможной реализацией угрозы t_i, определяется формулой

$$r_i = q_i p_{ti} \,, \qquad (2.6)$$

из сопоставления выражений (2.4) і (2.6) следует равенство:

$$p_{ti} = \sum_{j=1}^{k_i} p_{a\,j} \,, \qquad (2.7)$$

из которого, принимая во внимание, что значение вероятностного параметра p_{ti} не может превышать 1, вытекает ошибочность правого неравенства в утверждении (2.5).

Причину возникновения этого противоречия можно выяснить, описав ситуацию <угроза t_i / атаки> с позиции теории вероятности.

Пусть $< v_0, v_1, ..., v_{ki} >$ – множество элементарных событий, связанных с возможностью наступления события t_i (реализацией угрозы t_i), причем v_0 – элементарное событие, заключающееся в невозможности реализации угрозы t_i, а события $v_1, ..., v_{ki}$ – успешные реализации атак $\alpha_1, ..., \alpha_{ki}$, вектор $P = [p_{a0}, p_{a1}, ..., p_{\alpha \mathrm{ki}}]$ составлен из вероятностей соответствующих элементарных событий, а условные вероятности наступления события t_i определены форму-

лами: $p(t_i / v_0) = 0$, $p(t_i / v_j) = 1$, $j = \overline{1, k_i}$. Если множество $< v_0, v_1, ..., v_{ki} >$ представляет полную группу событий (то есть вероятность $P(v_j \bigcap v_l) = 0$, $j \neq l$ и $\sum_{j=0}^{k_i} p_{aj} = 1$), то

$$p_{ti} = \sum_{j=0}^{k_i} p_{aj} p(t_i / v_j) = \sum_{j=1}^{k_i} p_{aj}$$

и, следовательно, в этом случае выражение (2.4) верное: риск, возникающий в результате возможности реализации угрозы t_i, является суммарным риском атак, а для определяемой по формуле (2.7) вероятности реализации угрозы справедливо неравенство: $p_{ti} = 1 - p_{a0} < 1$.

Однако в общем случае две или более атак могут осуществляться совместно (комплексно). Это объясняется тем, что вероятность успешной реализации угрозы t_i путем проведения комплексной атаки выше, чем путем отдельной реализации любой из атак, входящей в состав комплексной атаки. Множество $< v_0, v_1, ..., v_{kj} >$, ввиду возможности совместных атак, уже не является полной группой и для расчета рисков в этой ситуации в [20, 23] рекомендуется трансформировать исходное множество элементарных событий $\langle v_0, v_1, ..., v_{kj} \rangle$ в множество комплексных событий, составляющих полную группу, рассчитать вероятности полученных комплексных событий (атак), соответствующие им потери, частные риски потерь вследствие реализации комплексных атак и, наконец, риск, связанный с реализацией угрозы t_i, который обобщает частные риски атак.

Например, из исходного множества атак $< \alpha_1, \alpha_2 >$, допускающих свое совмещение, формируем полную группу из четырех комплексных событий $< v_1 v_2, v_1 \overline{v_2}, \overline{v_1} v_2, \overline{v_1}\,\overline{v_2} >$, где v_j и $\overline{v_j}$ составляют пару противоположных событий, рассчитываем вероятности этих комплексных событий: $p_{12} = p_{a1} p_{a2}$, $p_{10} = p_{a1}(1 - p_{a2})$, $p_{02} = (1 - p_{a1}) p_{a2}$, $p_{00} = (1 - p_{a1})(1 - p_{a2})$, оцениваем соответствую-

щие значения потерь, считая, что $q_{12} = q_{10} = q_{02} = q_i$, $q_{00} = 0$. В итоге для угрозы t_i получаем абсолютно корректные соотношения: вероятность реализации угрозы t_i, представленная через вероятности атак, составляет:

$$p_{ti} = p_{12} + p_{10} + p_{20} = 1 - p_{00} = p_{a1} + p_{a2} - p_{a1}p_{a2},$$

соответственно риск угрозы t_i:

$$r_i = p_{12}q_{12} + p_{10}q_{10} + p_{20}q_{20} = (p_{12} + p_{10} + p_{20})\ q_i = q_i p_{ti}.$$

В общем случае реальные потери, возникающие при реализации каждой из комплексных атак, могут не совпадать друг с другом: $q_{12} \neq q_{10} \neq q_{02} \neq q_i$, $q_{00} = 0$. Тогда для угрозы t_i получаем риск $r_i = p_{12}q_{12} + p_{10}q_{10} + p_{20}q_{20}$, и далее из равенства (2.6) находим величину совокупных потерь, обусловленных реализацией угрозы t_i:

$$q_i = r_i / p_{ti}.$$

При существовании в ИС группы угроз $T = \{t_i\}$, $i = \overline{1,n}$, для которых условие несовместности обычно не выполняется, методика расчета обобщенного риска R (риска, обусловленного существованием различных опасностей, генерирующих все угрозы, которые действуют в среде функционирования ИС) практически ничем не отличается от уже рассмотренной методики обобщения рисков атак. В частности, из исходного множества угроз T формируется множество комплексных угроз, составляющих полную группу событий [20], объем N которой в общем случае определяется по формуле: $N = 2^n$. Исходя из заданного набора априорных вероятностей $\{p_{ti}\}$, $i = \overline{1,n}$, реализации каждой из множества исходных угроз $T = \{t_i\}$ рассчитываются вероятности реализации комплексных угроз P_{tl}, $l = \overline{1,N}$; из множества исходных потерь $\{q_i\}$, $i = \overline{1,n}$, обусловленных реализациями соответствующих угроз t_i, формируется множество совокупных потерь $Q = \{Q_{tl}\}$, $l = \overline{1,N}$, возникающих в результате реализации комплексных угроз. По полученным данным рассчитываются риски R_{tl}, $l = \overline{1,N}$ комплексных угроз, а затем, в соответствии с формулой (2.3), определяется их суммарный риск:

$$R = PQ_{\Sigma} = R_{\Sigma} = \sum_{l=1}^{N} R_{ti} = \sum_{l=1}^{N} P_{ti} Q_{ti} ,$$

который является характеристикой, обобщающей частные риски отдельных угроз, то есть интегральным риском группы угроз $T = \{ t_i \}$, $i = \overline{1,n}$. Полученное количественное значение интегрального риска позволяет оценить совокупные потери Q_{Σ}, обусловленные существованием в среде функционирования ИС различных опасностей, генерирующих множество угроз $T = \{ t_i \}$:

$$Q_{\Sigma} = R / P = R / (1 - P_{t0}),$$

где $P_{t0} = \prod_{i=1}^{n} (1 - p_{ti})$ – вероятность того, что ИС не подвергается влиянию каких-либо опасностей.

Приведенные выше материалы содержат рекомендации обще методического характера, суть которых сводится к формулировке требований, в рамках которых применение формулы суммарного риска (2.3) приводит к получению корректного результата. Как правило, на практике реализация этих требований сводится к необходимости трансформации исходной рисковой ситуации, возникшей в результате действий совокупности реальных деструктивных случайных совместных событий, в рисковую ситуацию, которая описывается полной группой комплексных событий, сформированных из исходного множества деструктивных событий. К сожалению, практическое использование этого подхода сталкивается с определенными трудностями. Чаще всего это связано с неопределенностью, появляющейся при оценивании величины потерь, обусловленных последствиями реализации множества деструктивных угроз. Описание, детализация и анализ некоторых из возникающих при этом ситуаций рассмотрен ниже.

Особенности описания и анализа рисковых ситуаций

В обобщенном виде рекомендации по процедуре оценки информационных рисков, актуальных для деятельности определенной организации, приводятся в соответствующих стандартах [8, 9] и подробно проанализированы в [24, 25]. Отмечается, что величина риска определяется уменьшением стоимости (ценности) активов

организации, обусловленным реализацией информационной угрозы t или совокупности угроз $T = \{t_i\}$. При этом в общей массе активов организации выделяются две группы: информационные активы ***IA*** и активы ***AS***, причем ко второй группе относят все активы организации (кроме активов ***IA***), ценность которых зависит от состояния активов первой группы.

К информационным активам ***IA*** (активы ИС) обычно относят элементы ИС, которые непосредственно используются для реализации тех или иных информационных технологий:

- информационные ресурсы ***IR*** организации – базы данных, файлы данных, системную документацию, руководства пользователя, архивированную информацию и т.д.;
- ПО: системное ПО, прикладное ПО, инструментальные средства, утилиты;
- физические активы ИС: компьютерное оборудование (процессоры, мониторы, периферийные устройства и т.п.), аппаратуру связи (телефонные станции, маршрутизаторы, модемы и др.), другое техническое оборудование, сооружения и помещения ИС;
- персонал и сотрудников ИС.

Состав активов ***AS*** (другие активы организации) существенно зависит от сферы, в которой работает организация, ее финансового состояния, подчиненности и т.д.

В частности, это нематериальные активы: репутация, имидж организации, уровень ее деловой активности. Сюда же следует отнести коммунальные активы: освещение, кондиционирование, обогрев, электропитания. Наконец, это могут быть продукция и услуги, производимые организацией, условия, определяющие выполнение работ организациями-смежниками, поставщиками и многое другое. Перечень активов второй группы может быть достаточно объемным, их отличие – зависимость стоимости этих активов от последствий реализации угрозы t_i, что выражается в:

- уменьшении уровня деловой активности организации;
- потерях / ухудшении репутации организации;
- финансовых потерях;
- приостановлении выполнения деловых операций;
- ухудшении инвестиционного климата;

– возникновении угроз личной безопасности персонала и т.д.

Рассмотрим оценивание риска реализации определенной угрозы t, ориентированной на поражение конкретного информационного ресурса ir_m. Механизм возникновения риска представлен на рис.2.4.

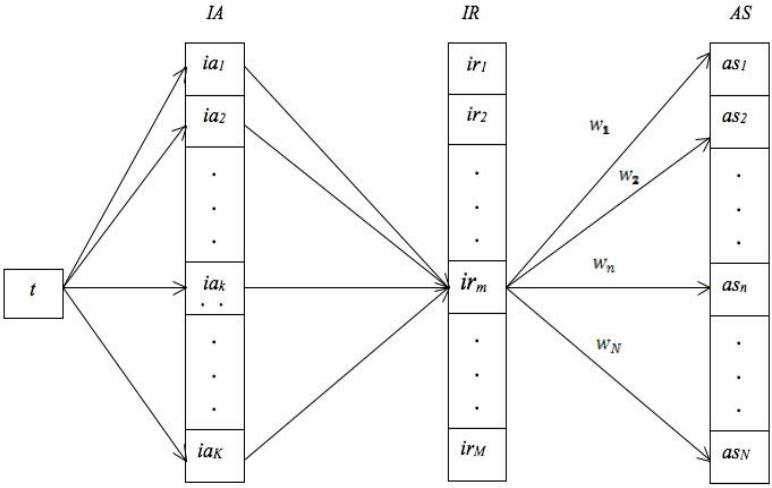


Рис. 2.4. Механизм формирования рисков, обусловленных реализацией угрозы t_i относительно информационного актива ir_m

Получить доступ к ресурсу ir_m можно только через те элементы ИС, которые непосредственно используются для транспортировки (передачи), хранения и обработки информации, представленной этим ресурсом, то есть через информационные активы ia_1, ia_2, ... , ia_K. Очевидно, что реализация угрозы *t* возможна только при наличии уязвимостей в этих активах, то есть путем проведения успешных атак, эксплуатирующих имеющиеся уязвимости, причем в общем случае у актива может быть несколько уязвимостей. Сначала оценим вероятность $p_t(ir_m / ia_k)$ успешной атаки ресурса ir_m через актив ia_k предполагая, что для актива характерны уязвимости, допускающие организацию атак $\alpha_0, \alpha_1, ..., \alpha_{l_s}$, вероятности успешных

реализаций которых представлены вектором $P=[p_{a0}, p_{a1},..., p_{al_s}]$. В этой ситуации оцениваемая вероятность определяется формулой:

$$p_t(ir_m / ia_k) = 1 - \prod_{j=1}^{l_s}(1 - p_{aj}). \qquad (2.8)$$

В общем случае, принимая во внимание, что угроза может одновременно реализовываться через существующие уязвимости информационных активов ia_1, ia_2, ... , ia_K, причем у каждого актива может быть несколько уязвимостей (т.е. атаки, направленные против этих активов, могут быть совместными событиями), вероятность p_t реализации угрозы t определяется формулой:

$$p_t(ir_m) = 1 - \prod_{k=1}^{K}(1 - p_t(ir_m / ia_k)), \qquad (2.9)$$

где каждая из условных вероятностей $p_t(ir_m / ia_k)$, $k = \overline{1, K}$ рассчитывается по формуле (2.8).

Потери организации, обусловленные действием угрозы t, определяются степенью чувствительности отдельных активов организации к изменению состояния информационного ресурса ir_m в результате реализации угрозы t, точнее, степенью и характером возникающих при этом искажений информации или компрометации информации, представленной данным ресурсом. Уровень потерь соответствует уменьшению общей стоимости этих активов (экономических, финансовых, имиджевых и т.п.), зависит от свойств и особенностей информационных технологий, принимающих участие в создании этих активов или в обслуживании их функционирования. Чем выше уровень информатизации организации, тем в большей степени ее активы зависимы от деструктивных воздействий на информационные ресурсы организации.

Введем обозначения:

- $Q(as_n)$ – стоимость актива as_n, $n = \overline{1, N}$,
- $w_n(t)$ – степень его чувствительности к воздействию (поражению действием) информационной угрозы t,
- $q(as_n / t) = w_n(t)Q(as_n)$ – величина потерь организации в результате реализации угрозы t относительно актива as_n.

В этом случае общие потери, понесенные организацией в результате реализации угрозы t относительно информационного ресурса ir_m, определяются формулой:

$$Q(ir_m / t) = \sum_{n=1}^{N} w_n(t) Q(as_n). \qquad (2.10)$$

Значения $w_n(t)$, $n = \overline{1, N}$ задаются расчетным, часто экспертным путем и обычно имеют вероятностный характер [26], представляя вероятность полной потери стоимости $Q(as_n)$ актива as_n в случае успешной реализации угрозы t относительно ресурса ir_m.

Зная значения потерь (2.10) и их вероятностную характеристику (2.9), находим величину риска организации для случая реализации угрозы, ориентированной на поражение информационного ресурса ir_m:

$$R_t(ir_m) = p_t(ir_m) Q(ir_m / t).$$

Принимая во внимание практические особенности рисковых ситуаций в реальных организациях, полученное частное решение следовало бы адаптировать к более общей постановке задачи.

Во-первых, следует учитывать, что рисковые ситуации зачастую создаются совместным действием ряда угроз $T=\{t_i\}$, $i = \overline{1, n}$, каждая из которых может осуществляться через некоторое множество информационных активов *IA*, поражая ряд информационных ресурсов *IR*. Это в свою очередь приводит к изменению состояния активов *AS* и в конечном итоге определяет уровень обобщенных потерь (рис. 2.5).

Во-вторых, кроме собственно трудоемкости и громоздкости анализа «траекторий» воздействия множественных угроз на активы организации, возникает проблема учета их взаимовлияния, точнее, учета последствий совместных деструктивных воздействий различных угроз на одни и те же активы *AS* организации. Обычно принимаемая в этом случае гипотеза аддитивности последствий может привести к неоправданному завышению объема интегральных потерь, в частности к абсурдному суммирования потерь взаимоисключающих последствий.

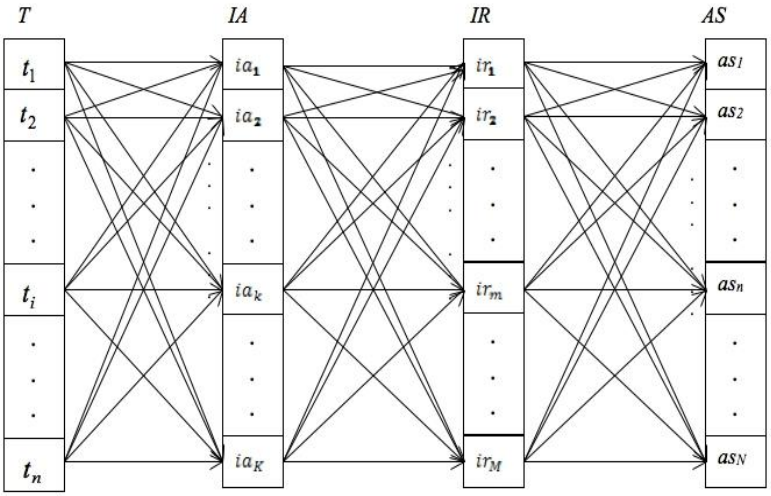


Рис. 2.5. Формирование потерь организации в условиях воздействия множества входных информационных угроз

К сожалению, для множества угроз при больших объемах активов достаточно сложно получить объективный вывод об уровне потерь путем поштучного рассмотрения влияния каждой из угроз на активы организации [27]. Приемлемый результат в этой ситуации может быть получен путем сведения последствий реализации любой из угроз к анализу трех характеристик (состояний) информационных потоков, циркулирующих в организации: доступности, целостности и конфиденциальности информации, из которой формируются данные потоки. Для этого составляется схема информационных потоков организации. В точках «введения» угроз (т.е. в уязвимых элементах информационных активов) определяется характер воздействия соответствующих угроз на состояние информации в той части потоков, которая проходит через точку «ввода». Затем оцениваются результирующие характеристики потоков и их влияние на состояние активов организации, которые «подпитываются» соответствующими потоками.

Эффективным приемом является также декомпозиция (фрагментирование) исходного множества активов *IR* на относительно неза-

висимые (функционально, организационно) подмножества [28], в пределах которых возможно практически автономное проведения АОР. В самом простом случае фрагментирование ресурсов *IR* влечет разделение исходной совокупности активов *AS* на отдельные подмножества, которые не имеют общих элементов и принадлежат к различным функциональным сферам: производственной, административной, управленческой и т.п., что существенно упрощает АОР.

Приоритизация информационных активов по степени их уязвимости

При проектировании и разработке систем защиты информации обычно оцениваются уровни деструктивного воздействия актуальных информационных угроз на объект риска ОР с последующей их классификацией по интенсивности своего влияния, что позволяет сконцентрировать усилия защиты на наиболее разрушительных угрозах. Однако, учитывая, что реализация любых информационных угроз осуществляется через уязвимости элементов информационных активов *IA* (рабочие станции, программное обеспечение, персонал ИС, технические средства и устройства связи и т.д.), при построении системы защиты ОР крайне полезны и необходимы сведения об интегральном уровне уязвимости отдельных элементов *IA*, входящих в состав ИС объекта риска. В частности, было бы желательно, чтобы этот интегральный показатель уязвимости обобщал значения группы рисков, происхождение которых связано с восприимчивостью определенного отдельного элемента *IA* к воздействию характерных угроз.

На рис. 2.6 приведена схема, иллюстрирующая процедуру оценивания интегрального уровня уязвимости информационного актива ia_k (сервера, маршрутизатора, прикладного программного обеспечения, администратора системы, авторизованные пользователя и т.п.) при его функционировании в составе ИС конкретной организации.

Согласно этой схеме, сначала путем предварительного анализа условий функционирования ИС объекта риска определяется сово-

купность угроз t_1, t_2, t_i, t_n, представляющих опасность для актива ia_k.

Далее по схеме информационных потоков организации определяется набор информационных ресурсов ir_1, ir_2, ir_m, ir_M, на которые через актив ia_k распространяется деструктивное влияние четырех вышеперечисленных угроз, и затем определяются элементы активов AS, критичные к воздействию искажений, уничтожению или компрометации информационных ресурсов ir_1, ir_2, ir_m, ir_M.

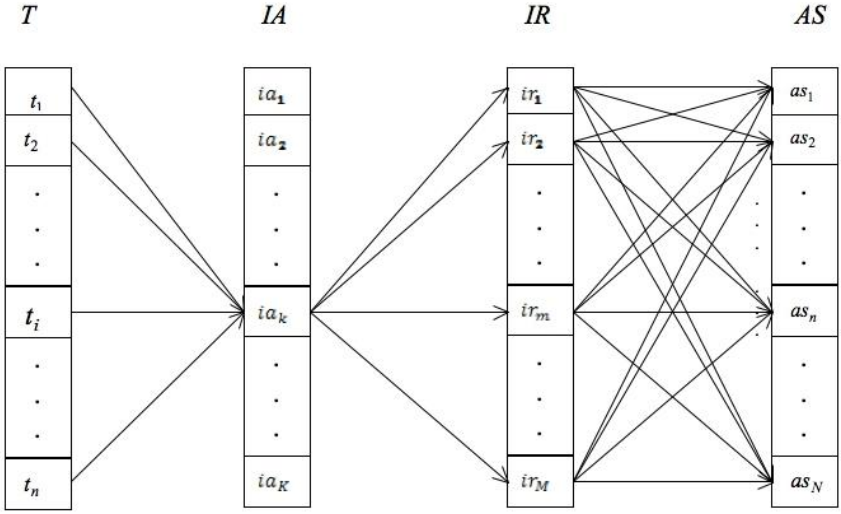


Рис. 2.6. Схема оценивания степени уязвимости информационного актива ia_k (в общем случае – это любой элемент *IA*: сервер, рабочая станция, прикладная программа, маршрутизатор, администратор системы, авторизованный пользователь и т.д.), который входит в состав ИС организации

Пусть $p_{ti}(ir_m / ia_k)$ – вероятность реализации одиночной угрозы t_i, использующей уязвимость информационного актива ia_k с последующим поражением информационного ресурса ir_m.

Степень чувствительности актива as_n к последствиям реализации угрозы t_i относительно информационного ресурса ir_m определим как $w_n(t_i, ir_m)$. Тогда значение риска потерь стоимости активов

организации, которые зависят от состояние ресурса ir_m, обусловленного уязвимостью информационного актива ia_k, будет составлять:

$$R(ir_m / t_i, ia_k) = p_{ti}(ir_m / ia_k) \sum_{n=1}^{N} w_n(t_i, ir_m) Q_n.$$

Обобщение рисков $R(ir_m / t_i, ia_k)$ по всем информационным ресурсам, подверженных воздействию угрозы t_i, приводит к выражению:

$$R(ia_k / t_i) = \sum_{k=1,2,m,M} p_{ti}(ir_m / ia_k) \sum_{n=1}^{N} w_n(t_i, ir_m) Q_n.$$

Степень чувствительности актива as_n к деструктивным последствиям реализации угрозы t_i определяется путем анализа схемы информационных потоков, поддерживающих те или иные информационные технологии, качество исполнения которых в свою очередь влияет на стоимость активов *AS* организации, и оценивается изменением (уменьшением) стоимости активов, вызванным искажениями или компрометацией информационных ресурсов вследствие реализации угрозы t_i.

Если предположить возможность выполнения раздельного анализа рисков реализацией каждой из угроз t_1, t_2, t_i, t_n, и считать справедливой гипотезу аддитивности последствий этих реализаций, то обобщенный риск организации, обусловленный уязвимостью информационного актива ia_k со стороны угроз t_1, t_2, t_i, t_n составит:

$$R(ia_k / t_1, t_2, t_i, t_n) = \sum_{l=1,2,i,n} [\sum_{k=1,2,m,M} p_{ti}(ir_m / ia_k) \sum_{n=1}^{N} w_n(t_i, ir_m) Q_n]. \quad (2.11)$$

Подобным образом можно оценить риски, обусловленные уязвимостями других информационных активов множества IA, и, про ранжировав эти риски, получить объективные сведения о степени приоритетности защиты тех или иных активов ИС.

Очевидно, что в первую очередь защите подлежат информационные активы IA, имеющие высокие уровни обобщенного риска (2.11) и, следовательно, наименее устойчивые к воздействию угроз

(или имеющие наибольшее деструктивное влияния на зависимые от их состояния активы AS и ресурсы организации).

2.3. Особенности анализа рисков в информационно-коммуникационных системах

Терминальные вероятности и динамические риски в ИКС

Если для традиционных автоматизированных систем управления (АСУ), в том числе АСУ ТП, стабильность состава производственных операций, неизменность требований к характеристикам выпускаемой продукции и относительная стабильность условий среды функционирования системы обусловливают устойчивость модели угроз и, как следствие, создание достаточно консервативной по своим параметрам системы защиты информации, то ситуация с защитой информационных ресурсов бизнес-процессов в информационно – коммуникационных системах (ИКС) диаметрально противоположна [29].

Особенностью бизнес-процесса является конечный цикл реализации отдельных бизнес-процедур, в ходе выполнения, которых применяются различные системы информационных технологий с присущими им индивидуальными особенностями, в том числе и уязвимостями в отношении угроз информации. Поэтому структура модели угроз бизнес-процесса является динамичной, ей присущи определенные особенности:

− непостоянство состава модели угроз для бизнес-процесса, его зависимость от конкретики поставленной задачи (задачи, которая решается, услуги, которая должна быть предоставлена);

− конечное время τ существования угроз, включенных в состав модели (как правило, связано с развитием бизнес-процесса, портфелем заказов, их продолжительности);

− распределение вероятности реализации каждой из угроз в пределах промежутка времени τ, соответствующего времени существования угрозы.

Последняя особенность обусловила введение в рассмотрение так называемой терминальной вероятности $P(t)$ реализации угрозы.

Терминальная вероятность $P(t)$ распределена на интервале времени по определенному закону [29, 30]:

$$P(t) = P_m \int_0^t p(t)dt = P_m \int_{t_1}^{t_1+t} p(t)dt$$

и соответствует значению вероятности $P(t)$ реализации угрозы за определенный промежуток времени $t \le \tau$, прошедший с момента начала реализации угрозы (*терминальная* от латинского *terminus* – предел, срок, определенный момент времени), причем $\int_0^\tau p(t)dt = 1$, а значит $P(\tau) = P_m$. При задании терминальной вероятности $P(t)$ в качестве функции плотности распределения $p(t)$ могут быть использованы как обычные виды распределений вероятностей, так и специфические, формы которых определяются конкретными особенностями ситуаций, возникающих в ходе развития событий в системе «атака–защита». Пример изменения терминальной вероятности $P(t)$ во времени приведен на рис. 2.7.

Момент возникновения угрозы – t_1, время ее существования – τ, $p(t)$ – плотность терминальной вероятности, равномерно распределенной во временном промежутке $[t_1, t_2]$, что обусловливает линейный характер роста в этом же промежутке терминальной вероятности $P(t)$ от 0 до максимального значения P_m с последующим сохранением своего значения до момента $t_1 + \tau$ завершения бизнес-процесса.

В момент $t_1 + \tau$ вероятность скачком падает до 0, что означает полное исчезновение у атакующей стороны интереса к информации, являющейся объектом атак. Пример подобной ситуации - проведение конкурса на лучшее решение некоторой задачи (проблемы) в условиях полной конфиденциальности проектов и их авторов.

В этом случае полуинтервалу $[t_1, t_2)$ соответствует время, в течение которого проходит сбор заявок на участие в конкурсе и подача проектов, интервалу $(t_2, t_1 + \tau)$ – обсуждение представленных проектов, моменту времени $t_1 + \tau$ – подведение итогов и объявление окончательных результатов конкурса.

Использование терминальных вероятностей позволяет учесть динамику развития атак, которая обычно остается «за кадром» при традиционном подходе к анализу угроз.

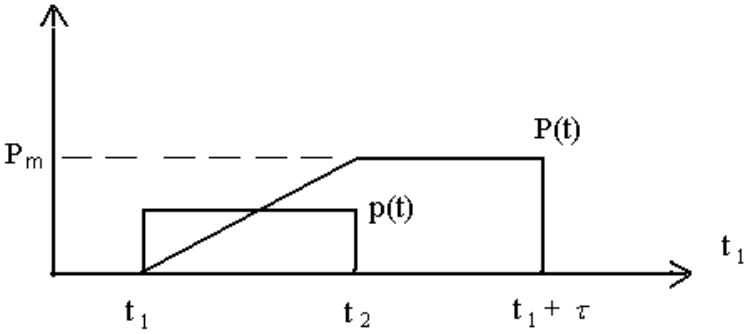


Рис. 2.7. Терминальная вероятность: зависимость значения вероятности $P(t)$ от плотности распределения $p(t)$ и времени τ существования угрозы

Рассмотрим предполагаемый сценарий развития некоторой угрозы, осуществляемой посредством проведения трех независимых атак: a_1, a_2, a_3, характеризующихся соответствующими вероятностями реализации: P_1, P_2, P_3. В условиях традиционного подхода к анализу этого сценария (т.е. не принимая во внимание распределенность атак во времени), учитывая, что атаки независимы, но совместимы и могут осуществляться как в одиночку, так и в комплексе:

$$<a_1, a_2>, <a_2, a_3>, ..., <a_1, a_2, a_3>,$$

можно сформировать из них полную группу событий, рассчитать вероятности этих событий, найти частичные риски от реализации всех возможных атак (в том числе комплексных) и оценить для полной группы событий интегрированный информационный риск [20, 24], характеризующий уровень защищенности информации.

Выполненный анализ рисков позволяет выявить наиболее опасные атаки, комплексы атак и оптимизировать процесс защиты информации. Однако в этом анализе не учтен временной фактор, отражающий обязательное существование интервалов времени, необ-

ходимых для развития и реализации каждой из атак. При этом вероятности P_1, P_2, P_3, воспринимаемые обычно как «точечные», на деле оказываются распределенными каждая вдоль своего интервала существования. Особенности соответствующих распределений и продолжительность интервалов могут весьма существенно влиять на построение и реализацию плана защиты.

В частности, каждой из атак a_1, a_2, a_3, можно поставить в соответствие свою терминальную вероятность $P_i(t)$, i=1, 2, 3, которая характеризует динамику развития атак во времени и при случае позволяет графически отобразить эту динамику или даже представить ее в форме математической модели (рис. 2.8). Для последнего случая в общем виде математическую модель можно описать выражением $P_i(t) = P_i \int_0^t p_i(t)dt$, где P_i – исходная «точечная» вероятность, $P_i = P_i(\tau)$. Очевидно, что для конкретной атаки успех ее проведения будет определяться степенью завершенности атаки, то есть продолжительностью срока ее развития и видом плотности вероятности $P_i(t)$ (рис. 2.9). В рассматриваемом примере, если предположить, что $P_1 \approx P_2 \approx P_3$, терминальная вероятность $P_3(t)$ для малых значений t может оказаться значительно выше аналогичных вероятностей двух других атак.

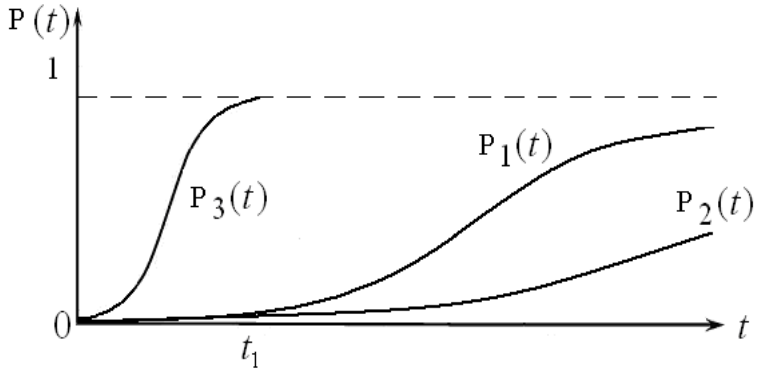


Рис. 2.8. Изменение во времени терминальных вероятностей $P_i(t)$, i=1, 2, 3, характеризующих динамику развития атак

В частности, учитывая, что для t_1 справедливое соотношение: $P_3(t_1) >> P_1(t_1) > P_2(t_1)$, стратегия управления защитой окажется существенно отличной от той, которая следует из традиционного формального анализа рисков (то есть без учета развития терминальных вероятностей во времени, только с привлечением «точечных» вероятностей P_1, P_2, P_3).

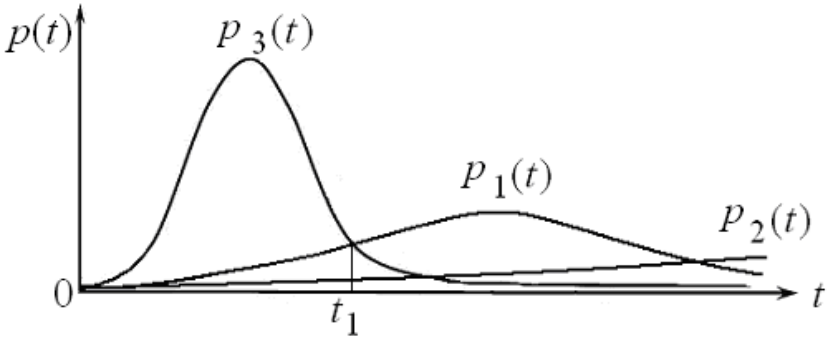


Рис. 2.9. Распределения плотностей вероятностей $P_i(t)$, *i*=1, 2, 3.

Приведенный выше пример позволяет предположить недостаточную корректность традиционной процедуры выделения существенных угроз (атак), которая сводится к ранжированию рисков угроз (атак) и сопоставлению их с фиксированным пороговым уровнем, равным минимально допустимому значению риска. Измеряемые риски в этой процедуре основаны на «точечных» вероятностях, тогда как объективность результатов ранжирования и парного сопоставления с порогом может быть обеспечена только в случае применения терминальных вероятностей, вычисленных для конкретного момента времени, которые учитывают фактическую распределенность «точечных» вероятностей в пределах интервала времени проведения атаки.

В общем случае величина терминальной вероятности монотонно возрастает с увеличением значений времени *t*, однако особенности и темпы этого роста определяются формой зависимости *P(t)*, которая учитывает динамику нарастания уровня обеспечения комплекса условий, гарантирующих успешное осуществление атаки. В качестве модельных распределений вероятности *P(t)* можно использо-

вать традиционные виды распределений, представленных типичными законами: равномерным, нормальным, лапласовым и т.п. Однако при этом, несмотря на конечность времени τ, все распределения будут усеченными как слева (для начальных значений переменной *t*), так и справа, в сторону возрастания времени *t*.

Очевидно, что если вероятности реализации угроз информации в ИКС характеризуются величинами, изменяющимися во времени (терминальными вероятностями), то и значение рисков ИКС, обусловленных существованием этих угроз, не могут быть постоянными во времени. Следовательно, как и вероятности, риски ИКС имеют принципиально динамический, процессный характер. При этом не исключено, что и второй компонент риска – убытки (потери), обусловленные реализацией угрозы, тоже меняются во времени.

В общем случае все это ведет к существенному усложнению анализа риска. Поэтому, если предположить, пусть в самом грубом приближении, возможность принятия гипотезы постоянства потерь, основная сложность анализа рисков будет связана с нахождением оценок терминальных вероятностей. В связи с этим ниже остановимся исключительно на вопросах оценки значений терминальной вероятности.

Сценарный способ задания терминальных вероятностей

Риск-аналитик часто заинтересован в максимально детализированном описании терминальных вероятностей, выделении в них отдельных составляющих, имеющих акцентированный самостоятельный смысл, связанный с особенностями или вынужденной временной фрагментацией реализации угроз.

Рассмотрим несколько вариантов (сценариев) развития событий, связанных с возникновением и развертыванием достаточно типичных угроз.

Как уже отмечалось выше, в ряде случаев вероятность реализации угрозы определяется по формуле [13, 14]:

$$P(t) = P_T(t)P_V(t),$$

где $P_T(t)$ – вероятность возникновения угрозы, $P_V(t)$ – вероятность реализации атаки, ведущая к осуществлению угрозы.

Рассмотрим ситуацию, возникающую при реализации атакующей стороной А (злоумышленниками) угрозы *T* относительно некоторого информационного ресурса *I*, принадлежащего стороне В. Считаем, что *D* – общая стоимость расходов атакующей стороны А на реализацию угрозы *T, g* – полученный при этом стороной А «выигрыш», определяемый ценностью информации *I* для злоумышленников [22, 26, 30].

Будем полагать, что активность стороны А в реализации угрозы *T* определяется в общем случае величиной чистой прибыли, которую сторона А может получить в случае успешной реализации угрозы *T*. Поэтому устойчивое стремление стороны А к осуществлению угрозы *T* количественно оценивается вероятностью возникновения (активации) угрозы.

Если предположить, что величина суммарных затрат *D*, понесенных атакующей стороной А в ходе подготовки, организации и проведения атакующих действий, является функцией времени, то вероятность P_T также будет зависеть от времени, то есть ее следует рассматривать как терминальную вероятность $P_T(t)$. В некоторый момент времени $t_{\max}$ величина суммарных затрат $D(t_{\max})$ достигает значения, при котором $D(t_{\max})/g$ становится равным 1, и в соответствии с формулой

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g},\ g \geq D,$$

терминальная вероятность $P_T(t_{\max})$ оказывается равной 0. Расходы $D(t_{\max}) = D_{\max}$ назовем предельно возможными затратами со стороны А (т. е. «злоумышленника»). Если текущие расходы δ атакующей стороны в среднем неизменны во времени, то справедливы соотношения:

$$D(t) = \delta t \leq D_{\max}, t_{\max} = D_{\max} / \delta,$$

где $t_{\max}$ – интервал времени, в течение которого сторона А полностью расходует свой атакующий ресурс и прекращает попытки реализации угрозы *T*. Тогда в соответствии с выражением

$$R_T = P_T q = P_t P_v q$$

терминальная вероятность $P_T(t)$ определяется формулой:

$$P_T(t) = (1 - \frac{\delta}{g} t).$$

Будем считать, что с ростом общего времени t, которое сторона А затрачивает на организацию, подготовку и проведение атак, растет терминальная вероятность $P_v(t)$ успешного использования им уязвимости V:

$$P_V(t) = p_v t,$$

где плотность вероятности $p_v(t)$ распределена равномерно в промежутке $(0, t_v)$, $t_v > t_{\max}$, то есть $p_v(t) = p_v = const$. Тогда вероятность реализация угрозы T определяется выражением:

$$P(t) = P_T(t) P_V(t) = (1 - \frac{\delta}{g} t) p_v t = p_v t - \frac{\delta p_v}{g} t^2.$$

При этом вероятность $P(t)$ растет от $P(0)=0$ до своего максимального значения $P(t_{extr}) = 0,25 p_V g / \delta$, которому соответствует момент времени $t_{extr} = g / 2\delta$. Затем вероятность $P(t)$ уменьшается снова до 0: $P(t_{\max})=0$.

Возможен такой вариант сценария развития событий в системе «атака-защита», при котором доминирующим становится влияние фактора времени на мотивацию и действия атакующей стороны А. В частности, предположим, что доступ к информации I возможен только в течение ограниченного полуинтервала времени $(0, t_m]$, то есть $P(t) = 0$ при $t > t_m$. В этой ситуации мотивация атакующей стороны А резко возрастает по мере приближения момента t_m (если все предыдущие попытки осуществления атаки закончились неудачей), что отображается моделью вида:

$$P_T(t) = \frac{P_{Tm}}{t_m - t + 1}, \; P_{Tm} = P_T(t_m).$$

Будем также считать, что предположения относительно характера и особенностей изменения во времени интервальной характеристики P_V остались прежними, то есть $P_V(t) = p_v t$. Тогда

$$P(t) = P_T(t) P_V(t) = \frac{P_{Tm}}{t_m - t + 1} p_v t.$$

Подобный сценарий характерен для развития событий, связанных с принятием стороной В некоторого критически важного для атакующей стороны А решение, заблаговременная информация о содержании которого жизненно важна для стороны А, в связи с чем расходы, обусловленные реализацией угрозы, отходят на второй план.

Особенности экспертного задания терминальных вероятностей. Байесовские оценки терминальной вероятности

Если выработки правдоподобных сценариев по какой-либо причине оказывается невозможной, выходом является экспертное задание значений терминальной вероятности. Крайне высокий уровень субъективизма экспертных оценок требует обязательного учета любых доступных достоверных сведений, позволяющих повысить надежность результатов, получаемых при обработке информации.

Особенно важным это проявляется при определении терминальной вероятности, процедура оценивания которой должна обеспечить постоянное обновление своих значений. Эффективный способ задания подобной процедуры может основываться на теореме Байеса, применение которой позволяет реализовать механизм согласования новых полученных данных о значении терминальной вероятности с ранее найденными. При этом процедура обновления с Байеса обеспечивает возможность интегрировать в новые оценки вероятности весьма приблизительные или даже противоречивые сведения [30].

Пример 1.

Предположим, что при анализе угроз информации в ИКС обнаружена некоторая угроза *T*, которая может быть осуществлена с помощью двух отличных друг от друга атакующих действий: атаки А и атаки В. Известны начальные оценочные значения вероятностей этих атак: априорное вероятность успеха атаки А равна p_a, атаки В - p_b. Анализ полученной новой оперативной информации свидетельствует об изменении значений исходных вероятностей, но при этом возникают две взаимоисключающие версии.

По одной из них, степень правдоподобности которой оценивается как p_1, на текущий момент реализована атака А, по другой – атака В (степень правдоподобности этой версии оценивается как p_2).

Исходная ситуация, которая первоначально сложилась с реализацией угрозы T, предполагает существование четырех гипотез (сценариев), составляющих полную группу событий и отражающих все априорно возможные варианты реализации угрозы T :

H_1 = < состоялась реализация только атаки А >, $P(H_1) = p_a(1-p_b)$;

H_2 = < состоялась реализация только атаки В >, $P(H_1) = p_a(1-p_b)$;

H_3 = < состоялась реализация обеих атак А и В >, $P(H_3) = p_a p_b$;

H_4 = < не состоялась реализация ни одной из атак >, $P(H_4) = (1-p_a)(1-p_b)$.

Событие Е, которое заключается в поступлении новой дополнительной информации о возможности осуществления атак А, В, меняет вероятности гипотез $H_1 - H_4$. Для определения их апостериорных значений прежде всего рассмотрим условные вероятности реализации события Е в соответствии с содержанием каждой из введенных выше гипотез:

$P\ (E/H_1)$ = < вероятность того, что полученная информация (событие Е) правдива относительно реализации атаки А, но ошибочна (ложна) относительно атаки В > $= p_1(1-p_2)$;

$P\ (E/H_2)$ = < вероятность того, что полученная информация (событие Е) правдива относительно реализации атаки В, но ошибочна (ложна) относительно атаки А > $= (1-p_1)p_2$;

$P\ (E/H_3)$ = < вероятность того, что полученная информация (событие Е) правдива относительно реализации обеих атак А и В > $= p_1 p_2$;

$P\ (E/H_4)$ = < вероятность того, что полученная информация (событие Е) ошибочна относительно реализации обеих атак А и В > $= (1-p_1)(1-p_2)$.

Приведенные выше условные вероятности позволяют рассчитать вероятность события E. В соответствии с формулой полной вероятности получаем:

$$P(E) = \sum_{i=1}^{4} P(H_i, E) = \sum_{i=1}^{4} P(H_i) P(E / H_i).$$

Теперь можно по формуле Байеса определить условные вероятности гипотез $H_1 - H_4$ после получения дополнительной информации (событие E):

$$P(H_i / E) = P(H_i) P(E / H_i) / P(E),\ i = \overline{1,4}.$$

В частности, если исходные данные принимают следующие значения: p_a=0,5, …, p_b=0,4, …, p_1=0,6, …, p_2=0,8, получаем:

$P(H_1) = 0{,}3,\ P(H_2) = 0{,}2,\ P(H_3) = 0{,}2,\ P(H_4) = 0{,}3,$

$P(E / H_1) = 0{,}12,\ P(E / H_2) = 0{,}32,\ P(E / H_3) = 0{,}48,\ P(E / H_4) = 0{,}08,$

$P(H_1 / E) = 0{,}164,\ P(H_2 / E) = 0{,}291,\ P(H_3 / E) = 0{,}436,\ P(H_4 / E) =$ 0,109.

Как видим, априорные значения вероятностей событий $H_1 - H_4$ существенно отличаются от их байесовских оценок. Если последние принять в качестве обновленных значений вероятностей $P(H_i),\ i = \overline{1,4}$, можно рассчитать обновленные значения вероятностей p_a, p_b, которые составят соответственно 0,601 і 0,727. При новом поступлении дополнительных оперативных сообщений (то есть при получении уже сверхновой информации, которая составит событие E_2) обновленные (уточненные) условные вероятности событий $H_1 - H_4$ следует рассматривать как априорные, которые могут быть вновь обновленные (повторно) путем применения уже рассмотренной выше процедуры пересчета по формуле Байеса. Очевидно, что в условиях поступления очередных дополнительных оперативных сообщений процедура пересчета предварительно обновленных значений вероятностей будет повторяться вновь и вновь, то есть она имеет рекуррентный характер.

В общем случае количество возможных способов реализации атак может быть больше двух, что приведет к увеличению количества возможных гипотез (сценариев) реализации угрозы, росту состава полной группы событий и, соответственно, к определенном

усложнению расчетов. В этой ситуации интересна возможность разделения любого сообщения на «атомарные» фрагменты, минимальные в некотором смысле по количеству информации, которую они содержат.

Пример 2.

Будем считать, что в условиях задачи, рассмотренной в **Примере 1,** «атомарное» сообщение должно нести информацию только о реализации угрозы путем проведения только одной атаки. Тогда исходное сообщение в рассмотренном выше примере фрагментируется на два «атомарные» сообщения, которым будут соответствовать две «атомарные» события: E_1 – на текущий момент получена информация (уровень доверия к ней p_1) о реализации атаки А, E_2 – на текущий момент получена информация (уровень доверия к ней p_2) о реализации атаки В. Фактически эта ситуация совпадает с ситуацией поочередной реализации во времени событий E_1, E_2, например, событие E_1 произошло в момент времени t_1, событие E_2 – в момент, $t_1 < t_2$.

Механизм поочередного учета этих сообщений не содержит ничего принципиально нового по сравнению с уже рассмотренным выше примером и состоит в двукратном последовательном применении процедуры пересчета данных по формуле Байеса. Назовем такую процедуру **типичной процедурой обработки «атомарного» фрагмента** информации (ТПОАФ) и рассмотрим ее содержание детальней на примере учета дополнительной информации, полученной к моменту времени t_1.

Для момента t_1, в зависимости от содержание введенных выше гипотез $H_1 - H_4$, определим условные вероятности реализации события E_1 совместно с каждой из этих гипотез $H_1 - H_4$:

$P(E_1/H_1)$ = < вероятность того, что полученная информация (событие E_1) правдива относительно реализации атаки А > = p_1;

$P(E_1/H_2)$ = < вероятность того, что полученная информация (событие E_1) ложна относительно реализации атаки А > = $1 - p_1$;

P (E1/H3) = < вероятность того, что полученная информация (событие E1) правдива относительно реализации атаки A > $= p_1$;

P (E1/H4) = < вероятность того, что полученная информация (событие E1) ложна относительно реализации атаки A > $= 1 - p_1$.

Выполненный расчет дал следующие результаты:
$P(H_1) = 0{,}3,\ P(H_2) = 0{,}2,\ P(H_3) = 0{,}2,\ P(H_4) = 0{,}3$ (очевидно, что априорные вероятности гипотез должны равняться соответствующим значениям вероятностей, исчисленным для первого примера),
$P(E_1 / H_1) = 0{,}6,\ P(E_1 / H_2) = 0{,}4,\ P(E_1 / H_3) = 0{,}6,\ P(E_1 / H_4) = 0{,}4.$

Итоговым результатом реализации ТПОАФ для момента времени t_1 являются апостериорные (уточненные) условные вероятности
$P(H_1 / E_1) = 0{,}36, \quad P(H_2 / E_1) = 0{,}16, \quad P(H_3 / E_1) = 0{,}24,$
$P(H_4 / E_1) = 0{,}24.$

Для момента t_2, учитывая, что полученные выше условные вероятности $P(H_i / E_1),\ i = \overline{1,4}$ следует воспринимать в качестве априорных, вновь проводим ТПОАФ, в результате которой получаем:
$P(H_1) = 0{,}36,\ P(H_2) = 0{,}16,\ P(H_3) = 0{,}24,\ P(H_4) = 0{,}24,$
$P(E_2 / H_1) = 0{,}2,\ P(E_2 / H_2) = 0{,}8,$
$P(E_2 / H_3) = 0{,}8,\ P(E_2 / H_4) = 0{,}2,$
$P(H_1 / E_2) = 0{,}164,\ P(H_2 / E_2) = 0{,}291,$
$P(H_3 / E_2) = 0{,}436,\ P(H_4 / E_2) = 0{,}109.$

Сравнивая расчетные результаты значений условных вероятностей $P(H_i / E_2),\ i = \overline{1,4}$ с результатами вычисления значений соответствующих условных вероятностей $P(H_i / E)$ для первого примера, констатируем их полное тождество, то есть имеем расчетное подтверждение эквивалентности рекуррентной обработки последовательности «атомарных» сообщений одноразовой обработке полного исходного сообщения, из которого путем фрагментации которого было получено ряд «атомарных». Справедливость этого предположения вполне очевидна, если учесть, что условные вероятности $P(E / H_i)$, принимая во внимание особенности рекуррентной

процедуры обработки как серии последовательно выполняемых ТПОАФ, представима в виде произведения

$$P(E / H_i) = P(E_1 / H_i)P(E_2 / H_i), \qquad (2.12)$$

что опять-таки легко проверить расчетным путем. Если количество «атомарных» сообщений будет больше двух, соответствующим образом увеличится длина серии последовательно выполняемых ТПОАФ и количество множителей в правой части соотношения (2.12).

Обобщая приведенные выше результаты на случай учета информации, полученной на момент t_k (событие E_k, уровень доверия к нему p_k), приходим к соотношениям:

$$P(E_k, H_i) = \frac{P(H_i)\prod_{j=1}^{k-1} P(E_j / H_i)}{\sum_{i=1}^{n} P(H_i)\prod_{j=1}^{k-1} P(E_j / H_i)},$$

$$P(E_k) = \frac{\sum P(H_i)\prod_{j=1}^{k} P(E_j / H_i)}{\sum_{i=1}^{n} P(H_i)\prod_{j=1}^{k-1} P(E_j / H_i)},$$

$$P(H_i / E_k) = \frac{P(E_k, H_i)}{P(E_k)} = \frac{P(H_i)\prod_{j=1}^{k} P(E_j / H_i)}{\sum_{i=1}^{n} P(H_i)\prod_{j=1}^{k} P(E_j / H_i)},$$

где n – количество гипотез в общем случае: H_i, $i = \overline{1,n}$, а условные вероятности $P(E_j / H_i)$ определяются выражением: $P(E_j / H_i) = p_j$, $j = \overline{1,k}$.

Отметим, что подобная рекуррентная процедура может быть применена к обработке новых оперативных поступлений информации любого объема и сложности в условиях предварительной фрагментации этой информации на «атомарные» сообщения, причем по своей структуре эти оперативные поступления могут вклю-

чать информацию, полученную от разных источников и в разные моменты времени. Определенные сложности возможны с интерпретацией вербально изложенного содержания новых поступлений информации. Например, сообщение E о том, что точно известно (то есть абсолютно точно, с уровнем доверия $p=1$), об успешной реализации угрозы T означает, что для условных вероятностей $P(E\ /H_i)$, $i=\overline{1,4}$, имеют место равенства:

$$P(E/H_1)=P(E/H_2)=P(E/H_3)=1,\ P(E/H_4)=0,$$

а сообщение о том, что достоверно известно об успешной реализации атаки, но только одной, означает, что для условных вероятностей $P(E/H_i)$, $i=\overline{1,4}$, должны выполняться равенства:

$$P(E/H_1)=P(E/H_2)=1,\ P(E/H_3)=P(E/H_4)=0.$$

В рассмотренных выше примерах пересчет (обновление) значений вероятностей происходил эпизодически, согласно поступлению новой оперативной информации об изменениях в состоянии атак. Однако, несмотря на то, что терминальная вероятность обычно «привязана» к определенному временному интервалу, целесообразно обновление оперативной информации проводить «принудительно», вводя мониторинговый контроль состояния атак (или ситуации с реализацией угрозы T). В этом случае оперативная информация должна поступать регулярно через определенный временной интервал.

Для современных ИКС, основой производственной и организационно-управленческой деятельности которых является бизнес-процесс, характерны неустойчивость структуры и состава модели угроз, конечное время существования угроз, изменение вероятности реализации угрозы в пределах времени ее существования и, как следствие, появление динамических рисков угроз. Кроме того, зависимость вероятности реализации угрозы от времени вызывает необходимость введения понятия терминальной вероятности и методов ее вычисления. Последние выше представлены сценарным методом определения значений терминальной вероятности и экспертно-аналитическим методом, в котором реализована возможность обновления ранее полученных экспертных оценок за счет учета (интеграции) дополнительных поступающих новых сведений.

СПИСОК ЛИТЕРАТУРЫ К ГЛАВЕ 2

1. А.Е. Архипов, В.П. Ворожко, «Задачи и проблемы обеспечения комплексных систем защиты информации», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 6, К., С. 137-140, 2003.
2. О.Є. Архипов, В.П. Ворожко, «Системний підхід до оцінювання ефективності захисту державної таємниці», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 10, К., С. 18-22, 2005.
3. «Risk management», Standard *AS/NZS 4360:2004*, Nundah : ISO working group – risk management Terminology, 2004, p. 65.
4. «International standard Risk management. Principles and guidelines», *ISO/FDIS 31000:2009(E)*, International Organization for Standardization, JISC, 2009, p. 24.
5. «Information security management systems. Guidelines for information security risk management» *BS 7799-3:2006*, International Organization for Standardization, 2006, p. 38.
6. «Systems and software engineering - Life cycle processes - Risk management», *ISO/IEC 16085:2006*, International Organization for Standardization, 2006, p. 34.
7. «Information technology. Security techniques. Code of practice for information security management. International standard», *ISO/IEC 17799:2005*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2005, p. 115.
8. О.Є. Архипов, *Вступ до теорії ризиків: інформаційні ризики: монограф*, К.: Нац. Академія СБУ, 2015, с. 248.
9. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», *ГОСТ Р ИСО/МЭК 15408-1-2008*.
10. «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]», *National Institute of Standards and Technology Special Publication 800-30*, Falls Church: Natl. Inst. Stand. Technol, 2002, p. 54.

11. Information Security Management. Part 2. Specification for Information Security Management systems. British Standard *BS 7799, Part 2. 2000*.

12. А. Алексеев «Управление рисками. Метод CRAMM», *IT Expert*, М.: ЗАО «ИТ Эксперт», 2010. [Online]. Режим доступа: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. [просмотрено 19 декабря 2010].

13. С.В. Симонов, «Методология анализа рисков в информационных системах», *Защита информации*, №2, С. 48-53. 2001.

14. С. Петренко, С. Симонов, *Управление информационными рисками. Экономически оправданная безопасность*, М.: Компания Ай-Ти, ДМК Пресс, 2004, с. 384.

15. И.М. Гостев, «Безопасность – бесполезная трата денег или их выгодное вложение?», *Конфидент. Защита информации*, №5, С. 16-18, 2003.

16. О.Є. Архипов, А.В. Скиба, «Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації», *Захист інформації,* Том15, №4, С.366 – 375, 2012.

17. А.Е. Архипов, «Применение рефлексивных моделей рисков для защиты информации в киберпространстве», *Захист інформації*, Том 19, №3, С. 204-213, 2017.

18. «Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards. LAWRENCE A.» *ISO/IEC TR 13335-4:2000*.

19. «Risk management.Code of practice and guidance for the implementation of BS ISO 31000», *BS 31100:2011*.

20. А.Е. Архипов, «Применение среднего риска для оценивания эффективности защиты информационных систем», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, науково-техн. Зб, Київ, Вип.1(14, С.60-67, 2007.

21. Lawrence Gordon and Martin P. Loeb «The Economics of Information Security Investment», *ACM Transaction on Information and System Security*, Vol.5, No4, November, P. 438-457, 2002.

22. А.Е. Архипов, «Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков», *Захист інформації*, №2 (51), С.69-76, 2011.

23. А.Е. Архипов, «Экспертно-аналитический подход к оцениванию информационных рисков», *Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції* (ISDMSI'2009), Том 1, Херсон: ХНТУ, С. 246-249, 2009.

24. А.Е. Архипов, А.В. Скиба, «Практические аспекты оценивания рисков реализации угроз в информационных системах», *Захист інформації*, Том16, №4, 2014.

25. О.Є. Архипов, О.Є. Муратов, *Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою, монографія*,. К: Наук.-вид. відділ НА СБ України, 2011, с. 195.

26. А.Є. Архипов, С.А. Архипова, «Применения мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита»», Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 1(16) вип., 2008.

27. О.Є. Архипов, «Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій», *Захист інформації*, №1 (50), С.42-47, 2011.

28. А.Е. Архипов, «Технология построения комбинированных измерительных шкал для оценивания значимости информации», *Адаптивные системы автоматического управления*, № 13(33), С.153–158, 2008.

29. А.Е. Архипов, «Об особенностях оценивания вероятностей, используемых для вычисления информационных рисков», *Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту*: Матеріали міжнародної наукової конференції (ISDMCI '2010), Том 2, Херсон: ХНТУ, С.515-517, 2010.

30. А.Е. Архипов, «Особенности анализа рисков в информационно-коммуникационных системах», *Захист інформації*, №4 (57), С.18 – 27, 2012.

Глава 3. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ В ОБЛАСТИ ОПРЕДЕЛЕНИЯ ЦЕННОСТИ ИНФОРМАЦИИ

3.1. Методические основы и способы определения ценности информации

Понятие ценности информации

Одним из базовых положений построения СЗИ является принцип разумной достаточности, согласно которому затраты на построение и сопровождение СЗИ должны сопоставляться с возможными потерями, имеющими место в случае реализации угроз относительно информации, подлежащей защите. Следование этому принципу позволяет оптимизировать затраты на создание СЗИ, обеспечив адекватность уровня защиты уровню ценности информации. Поэтому определение количественного значения ценности информации, которую надо защищать, является ведущим моментом процедуры оптимизации расходов на СЗИ [1]. Несколько конкретнее это положение сформулировано Мельниковым В.В. [2]: «Защите подлежит не всякая информация, а только та, что имеет ценность. Ценной становится информация, обладание которой позволяет получить какой-либо выигрыш: моральный, материальный, политический и т.д. ... Ценность информации является критерием принятия любого решения о ее защите». Содержание этого фрагмента достаточно убедительное с точки зрения актуальности и важности применения понятия **«ценность информации»** для построения и оптимизации СЗИ, однако суть самого понятие фактически не определена.

Следует отметить, что нет единого нормативного толкования термина «ценность информации», более того, часто его определения носят косвенный, опосредованный, иногда противоречивый характер. В пособии по информатике А.М. Морозевича [3] читаем: «Ценность информации проявляется в том случае, если она способствует достижению стоящей перед потребителем цели», в другом пособии [4]: «Ценность любого информационного источника определяется как разность между полезностями двух оптимальных стратегий, одна из которых обеспечивает свободу выбора различных действий для исходов, связанных с использованием информа-

ции, и вторая – в отсутствии такой свободы». Уважаемое академическое издание понимает ценность информации как «свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной человеческой деятельности для достижения определенной цели» [5]. Близкие приведенному, хотя и несколько измененные, ссуженные по содержанию объяснение термина «ценность информации» предоставляются в [6, 7].

Одним из главных вопросом практического применения понятия «ценность информации» является нахождение (вычисления) количественной оценки ценности информации. Эта проблема имеет давнюю историю. Ее исследованию посвящено значительное количество публикаций, в частности, работы К.Шеннона, О.О. Харкевича, Р.Л. Стратановича, М.М. Бонгарда и др. [8-13], которые стали классическими для этой области. Анализ приведенных в литературных источниках результатов позволяет утверждать, что существующее многообразие подходов и методов определения ценности информации объективно обусловлено существованием различных видов информационных систем, где обрабатывается или циркулирует оцениваемая информация, множеством несовпадающих целей, для реализации которых используется эта информация, особенностями прикладных задач, для решения которых она применяется.

Значение ценности информации не может быть получено путем прямого измерения, так как оно представляет собой так называемое латентное (скрытое) свойство, которое является ненаблюдаемым и неизмеримым непосредственно, поскольку к нему неприменима процедура измерения путем сопоставления с эталоном. Для измерения латентного свойства необходимо выразить его через измеряемые свойства, которые в этой ситуации называются индикаторами. Совокупность индикаторов, заменяющих латентное свойство (переменную), образует операциональный референт [9] или операциональный конструкт. Он используется вместо латентной переменной во всех зависимостях, в которые она входит. Операциональный конструкт должен быть валидным относительно своей латентной переменной, то есть должен достаточно точно воспроиз-

водить свойства, критические для всех применений, где задействована латентная переменная.

В простейшем случае операциональным конструктом может быть отдельный индикатор, в частности, для латентной переменной «ценность информации» – то, что позволяет количественно оценить пригодность определенной информации к ее конкретному практическому применению в том или ином виде деятельности. Очевидно, способ измерения значений выбранного индикатора будет зависеть от цели использования информации в каждом отдельном практическом применении. Это обусловливает появление множественности подходов и методов оценки уровней индикатора, о чем уже шла речь выше. Однако, если в качестве индикатора латентной переменной «ценность информации» взять полезность использования информации в различных прикладных приложениях и как одно из главных требований определить необходимость денежной формы представления значений этого индикатора, получим достаточно универсальный операциональный конструкт, независимый от способа «измерения» (вычисления) уровня полезности в каждом конкретном применении. Заметим, что анализ литературных источников, в частности приведенных выше [8-13], позволяет констатировать, что в большинстве случаев оценки ценности информации при соблюдении определенных дополнительных требований сводится именно к оценке полезности прикладных применений этой информации.

Это позволяет сформулировать следующее положение: «**Ценность информации измеряется уровнем максимальной полезности, полученной от привлечения оцениваемой информации к оптимизации выполнения определенного задания (выполнения работы, решения задачи, нахождение решения проблемной ситуации, оптимизации параметров производственного процесса и т.п.) при условии наилучшего способа использования этой информации»**. Некоторый экстремизм данного утверждения, содержащийся в оборотах «максимальная полезность», «наилучший способ использования», получил название принципа (условий) экстремальности [14, 15]. Очевидно, что польза от прикладного применения информации может быть различной. В первую очередь это зависит от потребителя информации, его знаний, умений, опыта,

возможностей понять, усвоить и удачно использовать полученную информацию. Поэтому полезность одной и той же информации может изменяться в широких пределах. Соблюдение принципа экстремальности подразумевает использование наиболее успешного варианта применения информации, соответственно – наивысшую (максимальную) полезность ее применения. Количественная оценка этой максимальной полезности и определяет ценность информации. То есть именно наличие принципа экстремальности в приведенном толковании **«ценности информации»** является залогом корректного однозначного количественного определения этой ценности.

Модели ценности информации

Формально ценность информации можно определить следующим образом [14-16]:

$$V(I) = \Delta A_{extr}(I) - d(I), \qquad (3.1)$$

где A – показатель, характеризующий степень успешности выполнения определенной задачи, работы, иного вида деятельности (этим показателем может быть стоимость продукции, изготовленной за определенное время или из фиксированного объема исходного сырья, выигрыш, обусловленный выбором удачного решения, общая стоимость услуг, предоставленных потребителям в определенной сфере деятельности и т.д.); $d(I)$ – расходы на получение, обработку и использование информации I в определенном виде деятельности; ΔA – улучшение (рост) показателя A за счет полученной информации I:

$$\Delta A(I) = A(I) - A_0,$$

где A_0 – исходное значение показателя (при отсутствии информации I), $A(I)$ –значение показателя A, достигнутое благодаря использованию информации I. В частности, значение A может увеличиться в результате применения полученной информации для оптимизации параметров производственного процесса, исключения возможных ошибочных или неперспективных вариантов решения определенной проблемы, рост имиджевой привлекательности данного вида профессиональной деятельности и тому подобное. Вы-

полнение условий экстремальности обусловливает рост показателя A до его максимально возможного значения A_{extr}, а именно до:

$$\Delta A_{extr}(I) = A_{extr}(I) - A_0.$$

В каждом конкретном применении информации I способ ее «потребления» будет разным: разовое использование информации I в задачах принятия решения для выбора наилучшего решения из множества возможных, распределенное во времени текущее использование информации для настройки параметров производственных процессов и т.п. Очевидно, наиболее приемлемая форма измерения значений V, A, d – денежная, хотя на практике используются условные единицы, баллы и др. В большинстве случаев величины V, A, d носят детерминированный характер и их значения могут быть точно вычислены по существующим нормативам и тарифам. Отметим, что приведенный способ вычисления уровня полезности информации, как и большинство других методов и подходов к определению ценности информации, базируется на парадигме позитивности последствий привлечения информации к оптимизации тех или иных видов деятельности.

Однако в задачах защиты информации эта парадигма не срабатывает, потому что в этой ситуации возникает отсутствующая ранее потребность в четком определении субъекта информационных отношений (владельца/потребителя информации или злоумышленника), с позиций которого определяется ценность информации. Например, для злоумышленника несанкционированный доступ к конфиденциальной информации I, легитимное право на ознакомление с которой у него отсутствует, в большинстве случаев стимулируется перспективой получения определенной прибыли, связанной именно с использованием этой конфиденциальной информации в своих интересах [17, 18]. Поэтому, для злоумышленника полезность этой информации I очевидна. Что касается владельца/потребителя информации I, то ситуация имеет двойной характер: во-первых, эта информация может быть полезна в традиционном смысле; во-вторых, компрометация информации I способна привести к убыткам, объем (стоимость) которых иногда может значительно превышать полезность, определяемую соотношением

(3.1). Это является достаточной мотивацией необходимости защиты информации, что также в каком-то смысле служит обоснованием ценности информации I. Поэтому, вопрос определения ценности информации, подлежащей защите, требует дополнительного рассмотрения.

Как известно из [6, 7, 16], потребительские качества информации в полном объеме гарантируются при условии обеспечения трех свойств информации:

− *доступности* (возможности получения санкционированным пользователем нужной ему информации не позднее заданного (малого) промежутка времени, защищенность ее от несанкционированного блокирования);

− *целостности* (защищенности информации от несанкционированного уничтожения, модификации);

− *конфиденциальности* (невозможности получения информации неавторизованным пользователем, защищенности от несанкционированного ознакомления).

Рассмотрим ситуации, возникающие при реализации угроз относительно этих трех приведенных свойств информации. Так, в случае разового использования информации I в задачи принятия решения, уничтожение или блокирование этой информации обусловливает невозможность роста показателя A, то есть $\Delta A = 0$. Это означает, что потребитель информации даром потратил деньги $d(I)$ на подготовку и обработку вовремя не использованной информации I, то есть фактически потерпел убыток. Добавив сюда упущенную выгоду, максимальный объем которой составляет $\Delta A_{extr}(I)$, получаем предельный объем ущерба потребителя:

$$l = \Delta A_{extr}(I) + d(I).$$

В случае использования текущей обновляемой информации, поступление которой распределено во времени, ее блокирования или уничтожения приведет практически к такому же ущербу, но с некоторым временным запаздыванием (лагом), в течение которого ущерб будет увеличиваться от 0 до l00% от своего предельного значения.

При модификации информации (при не выявлении факта ее модификации) или в случае разглашения конфиденциальной инфор-

мации убытки потребителя информации могут достигать существенных значений, превышая как $\Delta A(I)$, так и $A(I)$. При их оценке следует учитывать существование множества возможных сценариев развития событий [19], то есть эти убытки имеют принципиально вероятностный характер. Кроме того, в случае выявления факта модификации или компрометации конфиденциальной информации к общему объему убытков следует добавить расходы на восстановительные работы, связанные с ликвидацией последствий реализации соответствующих угроз информации.

В общем структура убытков, которые несет владелец конфиденциальной информации в случае реализации угроз относительно этой информации, имеет четыре составляющие:

$$L(I) = l_1 + l_2 + l_3 + L_\Sigma(I), \qquad (3.2)$$

где l_1 – расходы на создание и обработку конфиденциальной информации I (близкие или совпадающие с $d(I)$); l_2 – потери возможной прибыли из-за утечки конфиденциальной информации I (в ряде случаев совпадают с $\Delta A(I)$); l_3 – расходы на создание и эксплуатации СЗИ; $L_\Sigma(I)$ – интегральная оценка ущерба, являющаяся следствием возможных результатов развития негативных для владельца информации сценариев событий, обусловленных модификацией, утратой или разглашением конфиденциальной информации.

Отметим, что составляющая l_2 в случае, когда реализация угрозы информации не ведет к уничтожению или искажения информации, применяемой для оптимизации выполнения определенных задний (а, следовательно, они выполняются в неизменных условиях), может отсутствовать.

По своему характеру l_1-l_3 – детерминированные величины, значения которых (например, для действующей производственной системы) должны быть точно известны. Составляющая $L_\Sigma(I)$ – вероятностная величина, для вычисления требует знания пар $< p_j, L_j >$ – вероятностей развития каждого из возможных сценариев и результирующих убытков по каждому из них. Учитывая то, что в случае несовершенства или отсутствия СЗИ владелец конфиденциальной информации I может понести максимальный ущерб

в размере $L(I)$, именно эта величина принимается в качестве ценности $V(I)$ конфиденциальной информации.

Приведенные выше модельные соотношения основаны на упрощенном подходе к анализу ценности информации. Дальнейшее углубление исследований в этой сфере сталкивается с необходимостью рассмотрения и изучения ряда проблемных вопросов. Известно [4, 20], что ценность информации, в том числе и конфиденциальной, меняется со временем. Считается, что доминирует устойчивая тенденция к уменьшения ценности информации со временем, получившая название *процесса старения информации*. При этом в большинстве случаев в качестве адекватной модели процессов старения принимается экспоненциальная функция вида:

$$L(t) = L(0)(1 - e^{-\beta t}), \qquad (3.3)$$

где $L(0)$ – начальная ценность информации, коэффициент β – интенсивность старения информации, $1/\beta$ – среднее время старения.

Еще одной важной особенностью информации (как информации вообще, так и конфиденциальной) является нелинейная зависимость ее ценности L от объема этой информации. Пусть полный объем $I_{\max}$ конфиденциальной информации является достаточным для успешной реализации задач в определенной области человеческой деятельности. Ценность этого объема конфиденциальной информации составляет $L_{\max} = L(I_{\max})$. Если предположить, что определенный фрагмент этой информации объемом I попадет к злоумышленнику, максимальный уровень ущерба, который может быть нанесен владельцу информации, будет зависеть от того, насколько полно по этому фрагменту злоумышленник в состоянии восстановить содержание всей исходной информации $I_{\max}$. Если объем I близок к 0, восстановить по этим фрагментом исходную информацию практически невозможно даже в случае, когда к решению этой задачи злоумышленником привлекается опытный и хорошо подготовленный аналитик. Соответственно ценность такого фрагмента равна 0. Наоборот, если объем I близок к $I_{\max}$, ценность этого фрагмента фактически составляет $L_{\max}$, потому что очень вероятно, что специалист-аналитик получит все необходи-

мые для злоумышленника сведения из имеющегося фрагмента информации и ценность отсутствующей незначительной по объему информации $\Delta I = I_{\max} - I$ будет нулевой. Принимая это во внимание, можно предположить, что зависимость $L(I)$ – монотонно возрастающая на интервале (0, $I_{\max}$) функция, производная которой равна или близка 0 в начальной и конечной области этого интервала, но интенсивно растет в его средней части. Подобным требованиям удовлетворяет модель вида [16, 21]:

$$L(I) = L_{\max}\left[1 - \frac{1}{\beta_2 + (1-\beta_2)e^{\beta_1 I}}\right], \qquad (3.4)$$

где β_1, β_2 – коэффициенты, для значений которых выполняются условия: $\beta_1, \beta_2 > 0$, $\beta_2 \le 1$. Графическая иллюстрация зависимости (3.4) приведена на рис. 3.1. Следует отметить, что интенсивность роста переменной L зависит от уровня подготовки и интеллекта аналитика [1]. В модели (3.4) это отражается выбором значений коэффициентов β_1, β_2: рост значений β_1 смещает начало подъема графика $L(I)$ влево, в область малых значений I, а продолжительность «линейной» части графика регулируется подбором значений β_2, в частности растет с уменьшением этих значений и является короткой для значений β_2, близких к 1.

При недостаточной профессиональной осведомленности аналитика возможна ситуация, когда $L(I_{\max}) < L_{\max}$, причем разница $L_{\max} - L(I_{\max}) = \Delta L$ может оказаться достаточно существенной.

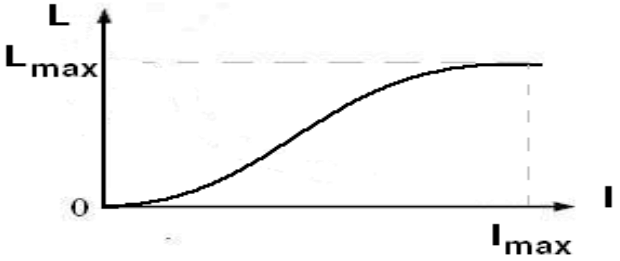


Рис. 3.1. Зависимость ценности информации L от её объема I

К сожалению, модели (3.3), (3.4) дают лишь общее представление о влиянии факторов времени и объема информации на ее ценность. Прикладное использование этих моделей, как и ряда других специфических модельных механизмов влияния различных факторов на ценность информации [2, 20], требует детализации и адаптации соответствующих моделей к условиям и особенностям конкретных приложений. На практике это крайне проблематично из-за недостаточной исследованности проблемы ценности информации. Некоторые предположения относительно происхождения, природы и особенностей зависимости ценности информации от ее объема приведены в работе [22], где анализируется наличие определенных генетических свойств секретной информации: если на базе этой информации образуется новая вторичная информация, она наследует особенности исходной информации и тоже будет секретной. Отмечается, что такой подход является достаточно упрощенным, так как если и прослеживается какая-то генетика, она имеет более сложный нелинейный характер.

Например, возможны ситуации, когда накопление открытой информации на определенной стадии этого процесса приведет к необходимости предоставления полученному собранию информации статуса секретной. Подобное утверждение приводится в [2], где отмечается, что совокупное количество или статистический свод несекретных данных в итоге могут получить гриф «совершенно секретно», то есть будет иметь место качественное преобразование совокупного массива информации, которое существенно выходит за пределы просто генетического наследования. Подтверждение возможности скачкообразного качественного преобразования накопленной информации, которое заставляет повысить степень ее секретности, описано в статье [1]. Приведенный в публикации пример базируется на материалах Свода сведений, составляющих государственную тайну Украины (ССГТ) [23], в частности на извлечении из содержания отдельной статьи ССГТ (см. табл. 3.1).

Как видно из этого извлечения, совокупная информация «в целом по Украине» безоговорочно получает гриф «особой важности», тогда как ее фрагменты могут иметь произвольный статус, хотя бы и несекретный, в зависимости от того, что решит в каждом конкретном случае государственный эксперт по вопросам гостайны.

Таким образом, именно собрание и общее представление совокупной информации может обусловливать резкий рост ее ценности.

Подобный эффект достаточно просто интерпретируется с позиций теории систем и системного анализа [24-26]: аналитическая совместная обработка всего комплекса (блока) информации систематизирует и упорядочивает накопленные в нем сведения и факты, позволяет выявить и формализовать совокупность связей и отношений между базовыми информационными элементами этого комплекса, то есть трансформировать исходную неструктурированную совокупность сведений в определенным образом упорядоченную систему взаимосвязанных компонентов с более или менее сложной структурой.

Табл. 3.1. Извлечение из ССГТ

Номер статьи ССГТ	Содержание сведений, составляющих государственную тайну	Степень секретности
1.9.2.	Сведения по отдельным показателям об открытиях, изобретениях, научно-технических решениях, которые могут быть использованы для нужд обороны страны и имеют принципиальное значение для разработки новых видов вооружения или военной техники	
	− в целом по Украине	«особой важности»
	− по отдельному открытию, изобретению или научно-техническому решению. По поводу отдельного открытия, изобретения или научно-технического решения: при засекречивании степень секретности устанавливается и снимается по решению государственного эксперта по вопросам тайн.	«совершенно секретно», «секретно»

Как известно, система характеризуется рядом свойств, среди которых одним из главных является **эмерджентность** – наличие у системы черт (свойств), которые не могут быть непосредственно выведены (полученные) по известным характеристикам отдельных элементов, составляющих систему [24-26].

Эмерджентность – следствие свойственного сложным системам **синергизма** [24], специфического эффекта взаимоусиливающих совокупных действий элементов системы, результат которых значительно выше простого суммарного эффекта от действия этих же элементов при их взаимонезависимом функционировании. В нашем случае следствие **эффекта эмерджентности** сведённых в единый информационный комплекс сведений – это существенный рост ценности такого совокупного информационного продукта за счет возможного применения к нему специальных технологий аналитической обработки, технологий анализа Больших Данных (Big Data), позволяющих извлечь в процессе совместной обработки большого объема данных информацию, ценность которой намного выше ценности результатов раздельной обработки частей этого информационного комплекса, полученных его фрагментацией на отдельные составляющие (единицы информации).

При обработке относительно небольших объемов узкоспециализированных данных ведущая роль в выделении ценной информации принадлежит аналитику. Однако при этом следует подчеркнуть, что при немашинной («ручной») обработке данных уровень эффективности упорядочения и систематизации изначально разрозненных единиц информации, составляющей исходный информационный комплекс, критически связан с уровнем знаний и индивидуальных умений аналитика. Последнее означает, что в зависимости от подготовки и способностей аналитика из одного и того же комплекса исходных данных можно получить множество возможных вариантов аналитических решений.

Рассмотрим иллюстративный пример [1, 16]: первичная информация – сведения о химических реагентах, ввозимых на территорию предприятия, о котором известно, что оно принадлежит оборонному комплексу. Эта информация вместе с определенной дополнительной информацией (каким образом транспортируют готовую продукцию, детали и элементы внешнего вида транспортной тары, вид и тип транспортных средств) образует информационный комплекс, результаты обработки которого в зависимости от качеств аналитика могут быть представлены несколькими вариантами заключения, различными по степени приближения к реальной ситуации:

а) предприятие производит компоненты, которые, возможно, применяются в снаряжении топливных систем военной техники;

б) предприятие является производителем ракетного топлива;

в) предприятие является производителем ракетного топлива для ракет типа XXXX;

г) предприятие является производителем ракетного топлива для ракет типа XXXX с приблизительным объемом производства YYYY тонн в месяц.

Возникает вопрос, какой степени секретности соответствует первичная информация, образующая информационный комплекс, обрабатываемый аналитиком. Многовариантность возможных результатов аналитической обработки первичного собрания информации усложняет задачу определения совокупной ценности сведений, составляющих информационный комплекс. Однако при классификации первичной информации с точки зрения ее возможной принадлежности к секретной, очевидно следует исходить из рассмотрения варианта, который ведет к наиболее тяжелым последствиям в случае потери информации. Появление этого варианта возможно при условии, что аналитик, работающий с первичной информацией, имеет наивысший уровень подготовки, и использует новейшие технологии обработки и анализа данных, которые позволяют ему максимально качественно трансформировать первичные данные в совокупность систематизированной и упорядоченной вторичной информации. Фактически здесь также применяется введенный выше принцип экстремальности, который позволяет избежать многовариантности. Однако, если бы каждому варианту из приведенной выше совокупности заключений можно было бы поставить в соответствие вероятность его получения, возможно следовало бы применить подход, базирующийся на применении аппарата средних рисков [27], который позволяет в итоговом результате учесть ценность информации по каждому из возможных вариантов путем введения специальной системы весов, где каждый вес пропорционален вероятности соответствующего варианта.

В любом случае, скорее всего совокупная ценность информационного комплекса окажется не соизмеримой с суммой ценностей отдельных единиц информации, из которых образован этот комплекс, существенно превышая эту сумму.

Данный пример отрицает правомерность применения достаточно распространенного на практике подхода, согласно которому ценность информационного комплекса исчисляется как сумма предварительно определенных ценностей отдельных единиц информации, игнорируя при этом существующую зависимость ценности единицы информации от ее объема, а также от объема и содержания уже накопленной ранее информации.

Таким образом, вычисление совокупной ценности информационного комплекса является нетривиальной задачей, общая методика решения которой до сих пор отсутствует, что обусловливает преимущественное использование экспертных методов решения этой задачи.

Информация: ценность или важность?

Выше для возможностей количественного оценивания латентной переменной «ценность информации» был введен операциональный конструкт, главную роль в котором играл индикатор «полезность информации». В формальной модели (3.1) значение этого индикатора определялось через показатель $\Delta A_{extr}(I)$ – максимальный прирост успешности выполнения определенного задания, обусловленный привлечением к его выполнению информации I. Однако в базовом соотношении (3.2), которое характеризует ценность конфиденциальной информации, индикаторами, формирующими операциональный конструкт, становятся убытки – антипод полезности. Этими индикаторами являются расходы l_1, l_3, «чистые» убытки $L_{\Sigma}(I)$ в интегральном представлении и убыток l_2 – упущенная прибыль, которую уместно было бы назвать «отрицательной (утраченной)» полезностью. В связи с этим ассоциация обобщающего (суммарного) ущерба $L(I)$ с понятием «ценность информации» является не совсем корректной. Возможно поэтому в некоторых источниках для определения данной обобщенной характеристики используют термины «важность информации» [2, 22], или «значимость информации» [28]. В частности, в [29]: важный – то, что имеет большое значение, от существительного waga (польск.) «вес, тяжесть», в переносном смысле «значимость», «ценность», то есть по своей содержательной нагрузке «важный»

шире, чем «ценный». Интересно, что в Законе Украины «О государственной тайне» от 21.09.1999р. №1079-XIV [2] для сравнительной характеристики свойств секретной информации применен термин «важность» (он же используется в обозначении наивысшей степени секретности – «особой важности»).

3.2. Практические аспекты определения ценности информации

Согласно украинскому национальному стандарту ДСТУ ISO/IEC TR 13335-3: 2003, ценность информации для организации определяется степенью зависимости эффективного функционирования организации от уровня и глубины вовлеченности этой информации в административно-управленческую и хозяйственно-производственную деятельность организации.

Таким образом, первое, что необходимо сделать для установления ценности циркулирующей в организации информации – оценить активы организации и степень влияния на них возможных инцидентов в сфере безопасности информации.

Обычно оценивание активов происходит в несколько этапов, первый из которых – этап инвентаризации (идентификации) активов. По результатам инвентаризации активов составляется перечень важных для организации активов, в котором можно выделить две группы: **активы системы информационных технологий (ИТ)** (другое название – **информационные активы**) и вторую группу – **другие активы организации**, куда вошли все остальные активы организации, ценность которых зависит от состояния активов первой группы.

К активам системы ИТ (информационным активам) обычно относят:

- информационные ресурсы: базы данных, файлы данных, системную документацию, руководства пользователю, архивированную информацию и т.д.;
- активы программного обеспечения: системное и прикладное программное обеспечение, инструментальные средства, утилиты;
- физические активы: компьютерное оборудование (процессоры, мониторы, модемы и т.п.), аппаратура связи (телефонные станции, маршрутизаторы, телефоны и т.д.), другое техническое оборудование, здания и помещения ИТС;

− персонал и сотрудники ИТС.

Состав активов второй группы (другие активы организации) существенно зависит от сферы, в которой работает организация, ее финансового положения, подчиненности и тому подобное. В частности, это нематериальные активы: репутация, имидж организации, уровень ее деловой активности. Сюда же следует отнести коммунальные активы: освещение, кондиционирование, обогрев, электропитания. Наконец, это могут быть списки работ, заказов, организаций-смежников, поставщиков, списки продукции, производимой организацией, и другое. В общем перечень активов второй группы может быть достаточно объемным. Чтобы его правильно сузить и одновременно не потерять что-то важное, оценке активов предшествует еще один дополнительный этап – определение границ инвентаризации активов [30]. Его задача – выделить те аспекты деловой деятельности организации, которые зависят от качества функционирования ИТС организации. С целью выявления этих аспектов, деятельность организации нужно проанализировать по двум группам критериев. Критерии первой группы позволяют выявить границы зависимости организации от ИТС и опираются на последствия анализа следующих положений:

− насколько важная часть бизнес-деятельности, которая требует обязательного привлечения ИТС;

− какие профильные (производственные) задачи организации могут быть реализованы только с помощью ИТС.

Вторая группа критериев направлена на выявление информации, которая нуждается в защите, и на анализ возможных последствий реализации угроз относительно этой информации:

− важные решения, принимаемые в организации, зависящие от точности, целостности, доступности и конфиденциальности информации, обрабатываемой в ИТС;

− какая обрабатываемая информация нуждается в защите, т.е. представляет собой критическую информацию;

− какие последствия могут возникнуть после инцидента, связанного с нарушением безопасности критической информации.

Закончив инвентаризацию активов, можно переходить непосредственно к установлению ценности активов. Основой для определения ценности может быть:

1) стоимость создания и обслуживания актива;

2) стоимость модернизации и восстановления актива;

3) ущерб, наносимый организации в случае нарушения конфиденциальности, целостности или доступности информационных активов;

4) комбинация трех предыдущих вариантов, что позволяет получить определенную интегральную оценку общей ценности актива.

Наиболее распространенным в практических применениях является способ вычисления ценности активов, в основе которого лежит третий из вышеприведенных вариантов. По этому поводу в стандарте ДСТУ ISO/IEC TR 13335-3 [30] отмечается, что расходы на активы (их прямая стоимость) – это лишь малая часть общей ценности активов. В частности, рекомендации по применению оценок убытков, обусловленных реализацией угроз относительно информационных активов, для определения их ценности для организации приведены в обязательных приложениях В, Е к указанному стандарту [30]. При анализе этого способа вычисления ценности активов надо принимать во внимание возможные последствия реализации угроз безопасности информации в ИТС, приводящие (среди прочего) к:

- снижению уровня деловой активности организации;
- потери/ухудшению репутации организации;
- финансовым потерям;
- перебоям в исполнении деловых операций;
- ухудшению инвестиционного климата;
- возникновению угроз личной безопасности и т.п.

После того, как будет составлен список, включающий полное множество активов организации: $AS = \{as_i\}$, $i = \overline{1, n_A}$, необходимо установить полный перечень возможных угроз информации $T = \{t_k\}$, $k = \overline{1, n_t}$ и проанализировать всю совокупность пар $< as_i, t_k >$, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$, вычислив в процессе этого анализа частичные убытки q_{ik}, обусловленные влиянием реализаций информационных угроз на состояние (качество функционирования, обеспечения стабильности, целостности и т.д.) каждого из активов. За-

тем по полученным частными убытками вычисляются окончательные совокупные значения ценностей соответствующих активов.

К сожалению, приведенной схеме нахождения ценностей активов присущ ряд недостатков [31].

Во-первых, это множественность получаемых для каждого актива оценок q_{ik}, количество которых определяется количеством тех угроз, последствия реализации которых ведут к потенциальным убыткам, требующим своего учета. Фактически каждая отдельная оценка q_{ik} отражает лишь частный ущерб, наносимый i-му активу as_i реализацией угрозы t_k. При реализации различных угроз пораженными могут оказаться как различные элементы, входящие в состав актива, так и такие, которые частично или полностью совпадают. Очевидно, формирование итоговой ценности актива в этих случаях будет происходить по-разному, исходя из информации о механизмах образования отдельных убытков, которая носит частный характер и может быть получена только при обследовании конкретной организации. В стандарте ДСТУ ISO/IEC TR 13335-3 [30] отмечается наличие проблемы множественности оценок активов, но отсутствуют какие-либо общие рекомендации по ее решению.

Во-вторых, в этом же стандарте (п. 9.3.3.) подчеркивается необходимость учета наличия взаимосвязей между различными активами при определении уровня ценности каждого из них, что объясняется существованием взаимосвязей определенных уязвимостей элементов ИТС организации и, соответственно, наличием взаимосвязей при реализации отдельных угроз информации. Также, как и в случае множественности оценок активов, учет взаимосвязей активов возможен только при наличии конкретной информации о частных особенностях и характеристики функционирования отдельных подсистем организации.

В-третьих, при больших значениях n_A и n_t (порядка нескольких десятков и более) множество пар $< as_i, t_k >$, $i = \overline{1, n_A}$, $k = \overline{1, n_t}$ становится достаточно большим, а процедура оценивания на базе этого множества окончательных совокупных значений убытков q_i, каждый из которых определяет ценность соответствующего i-ого акти-

ва as_i – чрезмерно громоздкой и трудоемкой. Действительно, нахождение окончательного совокупного ущерба q_i является результатом совместного анализа версий происхождения частичных убытков q_{ik}, $k=\overline{1,n_t}$, максимальное количество которых n_t в общем случае может значительно превышать рекомендуемый предельный объем 7±2 (известное число Ингве-Миллера [24], характеризующее ограниченность человеческих возможностей для эффективной совместной обработки воспринимаемых как одно целое ряда информационных фрагментов, каждый из которых в отдельности представляет собой совокупность фактов и связей). Кроме того, из-за необходимости исследования и анализа огромного количество пар $<as_i, t_k>$ эксперт вряд ли на деле сможет сознательно выделить и определить все частичные убытки q_{ik}, $i=\overline{1,n_A}$, $k=\overline{1,n_t}$, поэтому им сразу оценивается совокупный ущерб q_i каждого из активов, который и считается ценностью этого актива. Безусловно, прямое экспертное оценивание ущерба q_i, исключающее процедуру изучения и анализа частных убытков q_{ik}, значительно упрощает и ускоряет оценивание активов, однако при этом совершенно не учитывается механизм возникновения частных убытков, вследствие чего существенно возрастает уровень субъективных ошибок экспертизы.

Подчеркнем, что конечной целью, изложенной выше процедуры оценивания активов является определение уровня ущерба, нанесенного активам организации реализацией информационных угроз. Однако в этой процедуре фактически выпала из поля зрения сама информация, в отношении которой реализуются угрозы, и поэтому без внимания остается тот факт, что ущерб, нанесенный активам организации, образуется именно вследствие реализации угроз информации и зависит от важности последней для организации (то есть воздействия реализованных информационных угроз на обеспечение эффективного функционирования организации).

Поэтому целесообразно в процедуре оценивания активов организации более четко учесть причинно-следственные особенности процесса образования частных убытков и вычисление окончатель-

ного совокупного ущерба. При этом следует принимать во внимание три следующие аспекта:

− во-первых, точками ввода угроз в ИТС являются уязвимости активов системы, тогда как последствия реализации этих угроз нужно оценивать на полном множестве активов организации;

− во-вторых, на определенном этапе реализации любой угрозы информации эту угрозу можно свести к одной из трех: конфиденциальности, доступности и целостности, что позволяет упростить и сократить анализ последствий успешной реализации угроз, в том числе расчет соответствующих убытков;

− в-третьих, следствием реализации любой из этих угроз или их произвольной комбинации является поражение информации организации (точнее **информационных ресурсов** организации - совокупности упорядоченной определенным образом информации, зафиксированной на различных типах носителей, приспособленных для хранения и обработки этой информации в ИТС). Будем считать, что информационные ресурсы организации вместе составляют некоторое подмножество активов системы: $AS^{\inf} \subset AS$.

Формально с учетом указанных выше аспектов схему оценивания ущерба можно представить в виде трехэтапной процедуры [30]. При ее построении будем исходить из того факта, что в организации объектом приложения (ввода) угроз являются элементы информационной инфраструктуры (оборудование, программное обеспечение, персонал), которые из-за присутствующих в них уязвимостей делают возможной реализацию тех или иных атак в отношении информационных ресурсов. Последствия реализации этих атак (убытки организации) определяются на всем множестве AS активов организации.

На первом этапе процедуры оценивания убытков выполняется инвентаризация активов организации, результат которой - список активов, определяющий полное множество активов организации: $AS = \{as_i\}$, $i = \overline{1, n_A}$. Устанавливается перечень возможных угроз информации $T = \{t_k\}$, $k = \overline{1, n_t}$. формируется подмножество $AS^{\inf 1} \subset AS^{\inf}$, включающее только те информационные ресурсы

организации, относительно которых возможна реализация угроз из состава множества T.

В ходе второго этапа выполняется анализ всех возможных пар вида $\left\langle as_l^{\inf 1}, as_i \right\rangle$, по результатам которого определяются группы активов, ассоциируемые с каждым элементом $as_l^{\inf 1}$ информационных ресурсов, в отношении которых может быть реализована угроза. На третьем этапе, в ходе анализа всех возможных троек $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$, $i = \overline{1, n_A}$, выявляются убытки q_{ik}, наносимые активам as_i, $i = \overline{1, n_A}$ организации в случае реализации угрозы t_k относительно информационного ресурса $as_l^{\inf 1}$, и по совокупному значению всех этих убытков, исчисленных по всему множеству активов $AS = \{as_i\}$, определяют частную ценность соответствующего информационного ресурса $as_l^{\inf 1}$ (так называемая «присвоенная ценность» [30]).

К сожалению, как это уже отмечалось выше, при больших значениях n_A и n_t количество анализируемых пар $\left\langle as_l^{\inf 1}, as_i \right\rangle$, становится достаточно большим, троек $\left\langle t_k, as_l^{\inf 1}, as_i \right\rangle$ – еще больше, а процедура оценки значений q_{ik} – весьма громоздкой. Примером одного из самых экстремальных вариантов, которые могут возникнуть при оценивании активов, следует считать ситуацию, в которой организацией, чьи активы оцениваются, является государство. В этом случае множество пар <актив-угроза>, которые подлежат экспертированию, фактически бесчисленно, а значит применение изложенной выше процедуры оценивания активов является бессмысленной тратой времени. Для получения работоспособной процедуры оценивания активов в этом примере необходимо ввести механизмы сокращения количества анализируемых экспертом вариантов пар <актив-угроза> до разумного количества.

Одним из таких механизмов, подробно рассмотренным в [19], является метод сценарного анализа ущерба, обусловленного реализацией угроз в отношении определенного информационного ресурса (ИР). В этом методе эксперт для каждого вероятного случая реа-

лизации угрозы определяет конечное множество возможных сценариев развития событий-следствий (3-5 вариантов). Развертывание каждого из сценариев ассоциируется с некоторым конкретным множеством активов, которое по своему объему несравненно уже гипотетической полной группы активов. Поэтому эксперт способен достаточно объективно оценить последствия развития каждого сценария, которые фактически составят частные интегрированные оценки убытков (потерь), обусловленных реализацией исходной угрозы. В качестве окончательной оценки ущерба в случае реализации соответствующей угрозы можно принять наибольшую из частных оценок, полученных по каждому из сценариев, либо убытки по наиболее вероятному сценарию, или, наконец, средневзвешенный интегрированный ущерб по все совокупности сценариев, где весами являются вероятности реализаций каждого из сценариев.

Отметим, что рассмотренная выше схема оценивания активов достаточно универсальна с точки зрения возможных областей и диапазонов применения, однако в ряде случаев, характеризующихся наличием определенных ограничений в постановке задачи, эта схема оказывается излишне переусложненной.

Так, если целью оценки ИР является определение их принадлежности к секретной информации, множество угроз *T* фактически сужается к одной – угрозе утечки информации. Поэтому сразу отпадает проблема множественности оценок частных убытков, порождаемых реализацией многочисленных угроз информации. Объекты, в отношении которых может быть реализована угроза утечки - это множества ИР, которые обычно имеют определенные типовые документированные формы представления и устойчиво определенные области применения.

Последнее означает, что совокупность активов, которые функционально или иным образом связанные с атакованным ИР и им может быть нанесен ущерб, достаточно постоянна и характерна для всех ИР этой отрасли.

Поэтому, если в множестве подобных отраслевых ИР есть некоторая совокупность уже оцененных, эксперт может более-менее точно определить ценность всех ИР путем их сопоставления и сравнения с уже оцененными.

Точность полученных при этом оценок зависит как от уровня компетентности эксперта, так и способа (технологии), которая применяется им для сравнительного анализа и определения количественных значений ценности ИР. Одна из таких технологий предложена в [32], однако она не содержит детального описания механизмов своей реализации.

Поэтому ниже приведен пример адаптации этой технологии к анализу уровня ущерба, обусловленного реализацией угрозы утечки секретной информации.

3.3. Применение нониусного метода для определения ценности информации

Нониусный подход к определению ценности информации

Как уже упоминалось, базовым принципом построения СЗИ является тезис о разумной достаточности, согласно которому затраты на построение и сопровождение СЗИ не должны превышать приведенные к денежной форме представления суммарные потери, обусловленные реализациями возможных угроз относительно информации, подлежащей защите.

С другой стороны, возможности успешного, своевременного, полномасштабного и эффективного использования информации в организационной, производственной, социальной и других сферах деятельности организации зависят от выполнения требований целостности, доступности и, в ряде случаев, конфиденциальности циркулирующей в организации информации, т.е. от уровня ее защищенности, обеспечение которой реализуется системой менеджмента безопасности информации (СМБИ).

Недостаточная защищенность информации, подверженность ее деструктивным воздействиям информационных атак ведет к ухудшению качества функционирования организации в целом, показателем которого может выступать стоимость ее активов. Поэтому изменение (снижение) стоимости активов является характеристикой значимости информации для организации и именно эту характеристику целесообразно использовать при определении ценности информации (см. п. 3.1). Другими словами, ценность информации для организации оценивается величиной убытков, которые несет

организация в случае причинения вреда этой информации. Структура убытков определяется выражением (3.3), причем основные проблемы возникают при оценивании значения составляющей $L_{\Sigma}(I)$ – интегральной оценки ущерба, который несет организация из-за недоступности, модификации и/или утраты значимой для нее информации, утечки конфиденциальной информации. Для формирования представлений о методике определения ценности информации рассмотрим некоторые дополнительные сведения, касающиеся структуры активов организации.

По стандарту ДСТУ ISO/IEC TR 13335-3 [30], **активы организации** – это все, что имеет ценность для организации, причем ценность каждого актива определяется его важностью для деловой (функциональной) составляющей деятельности организации.

В частности, если речь идет о системе, например, ИТС, применяемой в пределах определенной организации, оценке подлежат прежде всего активы этой системы, причем при определении их ценности должно учитываться то, как может сказаться на ценности каждого из активов утечка, недоступность, искажения и/или разрушение информации, т.е. реализация основных видов информационных угроз по отношению к ресурсам ИТС организации.

На методологическом уровне принцип разумной достаточности реализуется в концепциях анализа и управления информационными рисками. Однако практическое воплощение этих концепций в процессе создания СЗИ требует решения ряда проблемных вопросов, один из которых – оценка ценности информации, в частности ИР, которые защищаются.

Актуальность этого вопроса наглядно подтверждается тем вниманием, которое уделяется ему в многочисленных нормативных и установочных документах [30, 33], причем практически все указанные документы в качестве основного механизма оценки ценности ИР определяют метод экспертно-аналитической оценки. В качестве примера можно взять стандарт ДСТУ ISO/IEC TR 13335-3 [30], в котором данный метод экспертизы ценности ИР используется в рамках так называемого «детального анализа рисков», представляющего собой один из вариантов корпоративной стратегии анализа рисков. Процедура экспертно-аналитического оценивания

каждого ИР базируется на системе критериев, в соответствии с которым совокупная оценка ценности ИР формируется из расходов на его создание (приобретение, обслуживание, восстановление) и возможных убытков организации-владельца ИР, обусловленных реализацией угроз конфиденциальности, целостности и доступности соответствующего ИР.

Вообще эффективное применение методики «детального анализа рисков» требует от эксперта глубоких знаний (как в сфере информационных технологий, так и в сфере деловой активности организации), значительных затрат времени и усилий. В связи с этим эксперты в своей практической деятельности часто отдают предпочтение так называемому «неформальному подходу» к анализу рисков [30], в котором экспертиза ценности ИР опирается не на структурно-аналитические методы анализа затрат и прогнозирования возможных убытков, а исключительно на собственный опыт и уровень осведомленности эксперта в соответствующей предметной области. При этом эксперт уходит от формированием оценки ценности ИР путем интеграции совокупности предварительно найденных фрагментарных (частных) оценок ценности отдельных единиц информации в одну обобщающую оценку, заменяя многоэтапную аналитическую процедуру экспертизы прямым определением конечной оценки. Подобное прямое экспертное оценивание дает существенную экономию усилий и времени, но вместе с тем существенно увеличивает вероятность появления субъективных ошибок в результатах экспертизы, в связи с чем регламентируются способы повышения точности результатов прямых экспертиз, например, путем рекомендаций по проведению групповой экспертизы. При этом на задний план уходит задача повышения точности индивидуальных экспертиз, которая сама по себе весьма актуальна и требует отдельного специального рассмотрения. В данном разделе рассматривается один из методов решения этой задачи.

Можно предположить, что эксперт, формулируя свои выводы в ходе прямой экспертизы, сознательно или подсознательно опирается на систему уже сложившихся у него представлений о ценности группы хорошо известных ему ИР, которые он считает базовыми в сфере данной профессиональной деятельности. Поэтому, формируя свою экспертную оценку относительно ценности представленного

на экспертизу нового ИР, эксперт пытается «вмонтировать» этот новый ИР в уже существующую систему базовых ресурсов и интерполирует его ценностный показатель по известным значениям ценности как «близких», так и «отдаленных» базовых ресурсов.

К сожалению процесс полученная этой интерполяционной оценки обычно оказывается вне сознательной фиксации его экспертом [34]. Тем не менее из литературы известны попытки построения эвристико-эмпирических процедур, цель которых – замещение эксперта в процессе формирования экспертного заключения путем применения подобной интерполяционной схемы или существенное упрощение продуцирования такого заключения.

В частности, в [16, 31, 35] предложен так называемый нониусный подход к определению ценности ИР, который позволяет постепенно конкретизировать класс, группу, подгруппу ресурсов, близких по определенным характеристикам к объекту экспертизы, последовательно сужая множество базовых ресурсов, сопоставляемых с новым ИР. Проиллюстрируем работу нониусной схемы. Предположим, что оценивается важность ресурса *IR*, содержание которого – данные контракта о поставках определенного вида военной техники в некоторую страну (рис. 3.2).

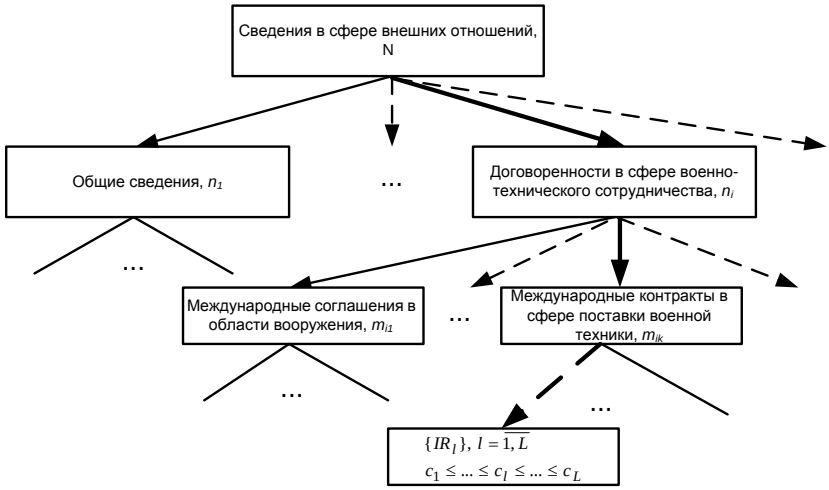


Рис. 3.2. Пример схемы классификации ИР в определенной предметной области

Общий объем документов в сфере внешних отношений составляет:

$$N = \sum_i n_i = \sum_i \sum_k m_{ik} = \sum_i \sum_k ... \sum_r L_{ikr} .$$

Согласно сути нониусного подхода, детализируя характер и особенности ресурса *IR*, постепенно спускаемся по ступеням иерархии рис. 3.2, редуцируя начальное множество из *N* анализируемых документов к содержимому определенной «атомарной» ячейки с ограниченным количеством базовых ресурсов $\{IR_l\}, l = \overline{1, L}$.

Считаем, что ценность c_l каждого из этих ресурсов уже известна и вместе они образуют конечное линейно упорядоченное множество $\{c_1, c_2, ..., c_L\}$. Для выработки решения по ценности c_{IR} ресурса *IR* эксперту нужно «втиснуть» этот ресурс в множество $\{IR_l\}$, и, ориентируясь по ценовым показателям элементов этого множества, определить ценность c_{IR}. Возможной формой оценки может быть взвешенная сумма [16, 35]:

$$c_{IR} = \sum_l w_l c_l ,$$

где w_l – система весов, задаваемых экспертом по результатам сопоставления ресурса IR с другими элементами множества $\{IR_l\}$ путем применением метода парных сравнений Саати [36] или другим способом. В дальнейшем оцененный ресурс IR вводится в множество базовых ресурсов.

Следует отметить, что условием реализации нониусного подхода является существование иерархии взаимосвязанных понятий, которая охватывает определенную предметную область. Именно наличие такой иерархии позволяет осуществить отнесения объекта экспертизы к требуемой подгруппе базовых ИР.

Еще одним примером прямого экспертного оценивания, близким по своей сути к нониусному подходу, является процедура присвоение грифа секретности секретной информации (СИ) [23]. Гриф секретности, размещаемый на материальном носителе СИ (МНСИ), должен соответствовать степени секретности СИ и определяется

путем сопоставления содержания этой информации с содержанием статей-описаний ССГТ [23], выявлением конкретной статьи ССГТ, содержанию которой соответствует информация, размещенная на МНСИ и присвоению этой информации грифа, рекомендуемого статьей ССГТ. Реализация поисковой процедуры обеспечивается иерархической структурой ССГТ, которая позволяет достаточно просто найти соответствующую статью-описание.

Онтологическая иерархия

В обоих приведенных выше примерах принятие решений базируется на использовании специфических иерархических структур - онтологий, изучению, разработке и применению которых в последнее время уделяется значительное внимание [37-40].

Онтология – это попытка всеобъемлющей и детальной формализации некоторой области знаний с помощью концептуальной схемы. Обычно такая схема представляет собой структуру данных, содержащую все релевантные классы объектов, их точные спецификации для определенной предметной области, связи и правила (теоремы, ограничения), принятые в этой области. Впервые понятие онтологии, как формального описания терминов, встречается в области изучения искусственного интеллекта. Однако, в последнее время данное понятие распространяется и на другие предметные области.

Потребность в разработке онтологий возникает в случае необходимости выполнения структуризации знаний в определенной предметной области для многократного повторного использования этих знаний или для их общего понимания совокупностью пользователей в различных сферах деятельности.

В простейшем случае построение онтологии сводится к выделению базовых понятий предметной области и установление соотношений между ними. Одной из проблем разработчика онтологии является необходимость выявления всех элементов, входящих в состав предметных областей. Вместе с тем онтологическая структура должна быть динамичной относительно изменений. Онтологии обычно строятся на анализе функциональных свойств и связей элементов определенной предметной области или на анализе содержания терминов соответствующей сферы, их сопоставлении.

Одним из примеров удачного применения и использования онтологического анализа можно считать ССГТ. В ССГТ все сферы деятельности разделены на четыре: сфера обороны, сфера экономики, науки и техники, сфера внешних отношений и сфера государственной безопасности и охраны правопорядка [23]. Соответственно, сфера обороны содержит основные спецификации понятий о виде вооруженных сил, округах, полках, отдельных воинских частях и тому подобное. Сфера экономики охватывает спецификации вопросов мобилизационных мощностей, создание государственных материальных резервов, формирования, финансирования и выполнения оборонного заказа и т.п. То же касается и других сфер деятельности. Все они содержат в себе определенные специфицированные понятия, которые в свою очередь раскрываются через еще более детализированные и конкретизированные категории. Фактически каждая из указанных сфер представляет собой частную онтологическую иерархию, поглощаемую более общей онтологической иерархией, корневым понятием которой является все множество сведений, составляющих ГТ. С другой стороны, любой элемент этой онтологической иерархии предполагает свое разложения в соответствующую частную иерархическую структуру.

Типичным образцом такого разложения является онтологическая иерархия (рис. 3.2), образовавшаяся из понятия **Сведения в области внешних отношений** (раздел ССГТ) и представляющая собой частную онтологию общей иерархической онтологии ССГТ. Меньшая по объему частная иерархическая структура подчинена ИР **Договоренности в сфере военно-технического сотрудничества**, еще более ограниченная – ресурсу **Международные контракты в сфере поставок военной техники**. Подчиненные иерархические структуры отсутствуют только для элементов самого низкого «атомарного» уровня онтологии ресурсов сферы внешних отношений.

Такой же подход можно использовать при построении онтологий и в других случаях, в частности для организаций, в том числе и коммерческих: всю совокупность данных, понятий, терминов или объектов, которые образуют предметную область в сфере функционирования соответствующей организации, надо категорировать, дать подробные спецификации этих категорий и указать их связи, воз-

можные подчиненности, зависимости. Для ССГТ эти категории разработаны государственными экспертами по вопросам тайн в процессе их многолетней работы, а эффективность полученной структуризации СИ подтверждена временем. Однако можно ли обеспечить надлежащее качество проведения онтологического анализа в более короткий срок, привлекая к этому не высококлассных экспертов, а специалистов разных уровней компетентности, которые не являются профессиональными экспертами или вовсе не имеют опыта проведения экспертиз? Как формализовать этот процесс?

Предположим, что объектом онтологического анализа является представленная в различных формах (в том числе и в виде совокупности ИР) информация, существование которой является необходимым условием устойчивого и качественного функционирования некоторой производственной организации, цель деятельности которой – создание (изготовление) определенного материального продукта (товаров).

Как известно, производство – это совокупность взаимосвязанных процессов: основных, вспомогательных и обслуживающих [41]. Основными процессами являются технологические процессы (ТП) производства, именно благодаря которым и образуется материальный продукт – основной результат производства. В связи с этим процесс формирования онтологической информационной иерархии производственной организации нужно начинать с анализа самых низких ступеней производства, то есть с определения информации, задействованной в основных производственных процессах (или бизнес-процессах, если производство не является материальным, например, если цель деятельности организации - оказания услуг). В частности, если речь идет об определенном материальном производстве, начинать надо с анализа его основных ТП.

На рис. 3.3 приведен фрагмент схемы ТП, представленного на уровне выполнения отдельных операций (кружки на схеме – выполнение соответствующих операций) [35].

Утолщенные стрелки на схеме указывают на потоки информации (I_1, I_2, I_3, I_6), отбор которой обеспечивает контроль параметров исходного сырья и материалов, задействованных в процессе производства, и характеристик состояния ТП. Это так называемая пара-

метрическая информация (данные обратной связи), которая передается от объекта к системе управления ТП.

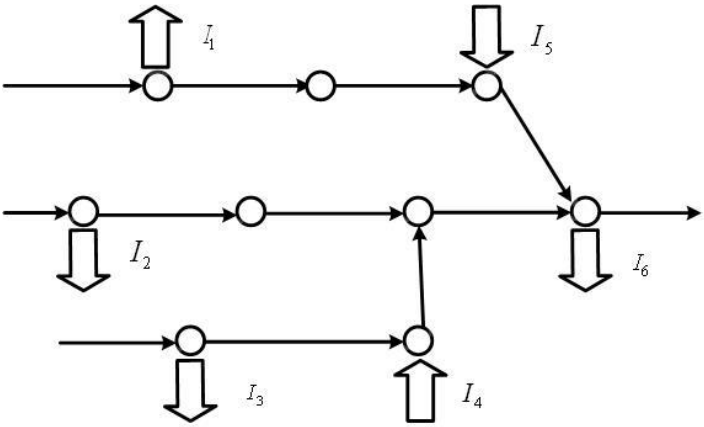


Рис. 3.3. Фрагмент схемы технологического процесса

По результатам обработки полученных данных система управления выдает информацию, которая передается каналом прямой связи (информационные потоки I_4, I_5) к объекту управления. Эта информация, меняя режимы работы сервисных устройств и оборудования, непосредственно связанных с регулированием состояния ТП, обеспечивает оптимизацию выполнения отдельных операций ТП и технологического цикла производства в целом. В общем всю перечисленную выше информацию можно обобщить единым понятием «технологическая информация».

Аналогичным образом можно проанализировать другие ТП, входящие в производственный цикл организации. Помимо различных фрагментов технологической информации основное производство будет характеризоваться информацией о выпуске конечного продукта, поставке и потребления сырья, энергоресурсов, количественных и качественных показателях производства в целом и т.д. Следует также отметить, что в рамках управления данным ТП реализуются связи со смежными ТП, обеспечивается ремонт оборудования, поставка инструментов и т.п. Кроме того, в состав организации должны входить обеспечивающие подразделения, в которых циркулирует финансово-экономическая информация, отчетно-

статистическая информация, сведения кадровой службы (включая соответствующие персональные данные), информация, связанная с разработкой, проектированием, технологической подготовкой и планированием выпуска новых видов продукции и тому подобное. Представленная в документированном виде, вся эта информация составляет внутренние ИР организации. Циркуляцию этих документов в организации обеспечивает система документооборота и архивное подразделение. Отдельный ИР формируется из информационных потоков, ориентированных во вне организации (внешняя информация). Это сведения о продаже и маркетинге, логистике и снабжении, налоговом учете и выплате налогов, внешнем инвестировании, портфеле заказов и т.п.В целом вся информация, перечисленная выше, представляет собой **Совокупную информацию организации**, которую можно представить в виде многоуровневой иерархии. На первом уровне выделим:

1. Внутренняя информация / 2. Внешняя информация.

Детализируя их, получаем элементы второго уровня иерархии:

1.1. Производственная информация / 1.2. Информация обеспечивающих подразделений

2.1. Сведения о продаже и маркетинге / 2.2. Отчетно-статистическая информация / 2.3. Рекламно-справочная информация / 2.4. Расчеты с поставщиками и получателями продукции / ...

Третий уровень иерархии:

1.1.1. Технологическая информация / 1.1.2. Документация по технологической подготовке производства;

1.2.1. Данные о бухгалтерском учете / Сведения об учете и управлении кадрами / Планово-финансовая информация / Административно-управленческая информация / Аналитико-маркетинговая информация / ...

. . . . . .

2.1.1. Сведения о поставщиках, объемах закупок и спецификации сырья, материалов / 2.1.2. Договоры с покупателями товаров, спецификации к ним / 2.1.3. Ведение ценовых структур, формирование прайс-листов / ...

. . . . . .

В тех случаях, когда это необходимо или целесообразно, возможно введение дополнительных уровней иерархии. Например: **1.1.1.1. Параметрическая информация: *I_1, I_2, I_3*, / 1.1.1.2. Информация прямого канала управления ТП: *I_4, I_5*.**

Степень детализации по направлениям онтологической иерархии индивидуальная для каждого из них и тесно связана с возможностью подсчета ценности информации соответствующего низшего уровня иерархии. Так, если самые низкие «атомарные» ячейки иерархии по направлению **1.1. Производственная информация** образуются элементами параметрической информации и информации прямого канала управления ТП, их ценность рассчитывается по потерям от блокирования или искажения (модификации) этой информации, приводящим к ухудшению качества продукта ТП, увеличению процента брака или остановке ТП.

В общем ценность технологической информации любого ТП (бизнес-процесса) определяется через оценку воздействия негативных последствий реализации угроз в отношении целостности и доступности этой информации на характеристики состояния ТП (бизнес-процесса), его устойчивость. При такой оценке учитывается косвенное влияние атак на информационные ресурсы через изменения в стоимости конечных продуктов ТП (на отдельных стадиях бизнес-процесса) и продукции производства в целом. В частности, для «атомарных» элементов информации I_1 – I_6 получаем частные оценки полезности (важности) каждого типа этой информации для обеспечения производственного процесса. Обобщение (объединение) информации I_1 – I_6 в категорию **1.1.1. Технологична информация** должно сопровождаться вычислением соответствующей совокупной оценки потерь от реализации угроз в отношении этой категории. В целом должны быть получены совокупные оценки влияния каждой из угроз по каждому обобщенному ИР (типизированной информационной категории) по всем подразделениям организации. Уместно заметить, что особенностью подобной процедуры определения ценности информации или ИР является то, что она происходит на начальном этапе анализа рисков, когда еще отсутствует детализация возможных для данной организации информационных угроз и способов их реализации.

Поэтому в соответствии с уже устоявшимся пониманием содержания понятия «ценность информации» реальная ценность информации (или ИР) определяется исключительно через оценки влияния нарушений доступности, целостности и конфиденциальности конкретной информации (ИР) на деятельность (состояние функционирования) организации, точнее через возможные потери организации в результате реализации этих нарушений.

Для внешней информации организации (как и для некоторых видов внутренней) часто характерны повышенные требования к ее конфиденциальности. Расчет возможных потерь в этом случае носит вероятностный характер и выполняется с привлечением ситуационно-сценарных методов прогнозирования [16, 19].

Подчеркнем, что приведенная выше методика построения информационной онтологии основана на выделении основных информационных элементов онтологии и установлении соотношений между ними путем анализа функционально-производственной структуры организации. Очевидно, что это не единственно возможный подход к формированию онтологии. В частности, можно надеяться на эффективное применение для построения онтологии так называемой информационной пирамиды, которая характеризует особенности и свойства информации, задействованной на разных уровнях управления организацией [42]: стратегическом, тактическом, оперативном.

Этот подход позволяет ввести в структуру онтологии достаточное количество информационных элементов, которые смогут более-менее полно представить предметную сферу, однако структура их взаимосвязей будет отличаться от соответствующей структуры, полученной при построении онтологии по функционально-производственному принципу.

Упрощение процедуры экспертного определения ценности информации при сохранении достаточно высокого уровня качества экспертных оценок можно получить при использовании так называемого нониусного подхода, уже рассматривавшегося выше. Однако возможность его применения требует предварительной структуризации информации в определенной предметной области (области деятельности). Удачной формой такой структуризации является построение онтологической иерархии информационных элементов

соответствующей сферы (отрасли) деятельности. Анализ существующих приложений информационных онтологических иерархий, их основных свойств и особенностей структуры обусловливает целесообразность использования в формировании информационной онтологической иерархии подхода, основанного на изучении и исследовании комплекса реализуемых в организации функционально-производственных процессов. Целью этих исследований является определение состава, содержания и взаимосвязей информации, чье наличие обеспечивает эффективное и устойчивое функционирование организации. Именно на базе этой информации формируется информационная онтология. Кроме того, исследование этих связей с позиций обеспечения устойчивости производственных процессов и качества конечной продукции допускает достаточно прозрачное определение ценности определенных информационных блоков, образующих разные уровни информационной онтологии.

3.4. Применение системы комбинированных шкал для оценки информационных потерь

Обобщенная задача измерения и типология комбинированных шкал для определения ценности (значимости) информации

Процедуры измерения сопровождают любого человека на протяжении всей его жизни и в большинстве случаев выполняются подсознательно (этот человек выше, тот – ниже; сегодня он в хорошем настроении / не в настроении; веселый / радостный / грустный / подавлен и т.п.), их результаты в основном не фиксируются, оставаясь обычно вне нашего внимания.

Именно поэтому, когда речь заходит об измерении, его ассоциируют с техникой, естественными науками и другими видами деятельности, где сутью измерения является сопоставление измеряемого качества (часто это геометрические, физические свойства исследуемого объекта) с соответствующим эталоном, причем в процедуре измерения широко применяются специальные измерительные технические средства и полученные результаты измерения имеют вполне объективный характер.

Однако во многих областях человеческой деятельности (экономика, социология, психология, другие социальные науки) един-

ственным измерительным средством, применяемым в процессе измерения, является сам человек, а в процедуру измерения, кроме чисто технических действий, вводятся элементы интеллектуальной деятельности. Например, изучая сложный социальный объект, исследователь может ввести определенную переменную, которая, по его мнению, отражает главные особенности этого объекта и может выступать в качестве интегральной характеристики объекта в целом.

Часто эта переменная не может быть измерена непосредственно, ее значения оцениваются исследователем, экспертами или определяются каким-то другим косвенным способом, имея при этом очевидно субъективный характер. В этой ситуации возникает потребность в разработке общей теории измерений, которая решила бы проблему унификации измерений на объектах различного происхождения, воссоздав общую формальную схему как объективных, так и субъективных измерений. Одна из первых работ, в которой была предпринята попытка построения общей теории измерений, базирующейся на теоретико-множественном аппарате отношений, принадлежит П. Суппесу [43].

Рассмотрим совокупность исследуемых объектов, принадлежащих к одному классу, интегральная характеристика которых отражается переменной x. Естественно, что для каждого *r*-го объекта в соответствии с его состоянием эта переменная имеет разную степень интенсивности x_r, то есть по всей совокупности объектов получим множество интенсивностей $X = \left\{ x_r, r = \overline{1,m} \right\}$. Зафиксируем структуру этого множества путем определения парных (бинарных) отношений между ее элементами, обозначая эти отношения выражением $q_{rk}(x_r, x_k)$ или просто q_{rk}. Совокупность всех возможных отношений удобно представить квадратной матрицей $Q = \left\| q_{rk} \right\|_{m,m}$. Назовем кортеж (двойку) $S = \left\langle X, Q \right\rangle$ эмпирической системой с отношением (ЕСО). Предположим, что возможно однозначное отображение

$$\gamma : X \to R, \tag{3.5}$$

где R – множество всех действительных чисел, в частности каждый элемент x_r можно сопоставить с числом $z_r = \gamma(x_r) \in R$.

Тогда все множество элементов X можно сопоставить с множеством $Z = \left\{ z_r, r = \overline{1,m} \right\}$, элементами которого являются действительные числа. Структуру множества Z определим через систему парных отношений d_{rk} аналогично тому, как это было сделано для множества X, представив совокупность этих отношений квадратной матрицей $D = \left\| d_{rk} \right\|_{m,m}$. Пару $C = \left\langle Z, D \right\rangle$ назовем числовой системой с отношениями (ЧСО). Если совокупность числовых значений ЧСО, образовавшихся в результате отображения (3.5), имеет такую структуру, для которой удовлетворяется условие $Q = D$, то система C представляет собой гомоморфный образ (гомоморфизм) системы S, а отображение

$$\gamma^* : S \to C,$$

называется гомоморфным.

Если отображение S является взаимно-однозначным, имеем случай изоморфного отображения (изоморфизм). То есть изоморфизм гарантирует единообразие структур систем, а гомоморфизм - их сходство. Кортеж (тройка) $\left\langle S, C, \gamma^* \right\rangle$ называется шкалой измерения.

В более узком смысле шкала – это совокупность правил, по которым выполняется сопоставление множества состояний эмпирического свойства изучаемого объекта множеству действительных чисел. Сам процесс сопоставления составляет процедуру измерения, определяющей особенностью которой является обеспечение (воспроизведение) между элементами числовой системы характера отношений между соответствующими состояниями эмпирического свойства.

Отметим, что одну и ту же ЕСО S можно отразить в числовую систему различными способами. В частности, если результатам таких отражений γ_1 і γ_2 являются ЧСО C_1 и C_2, в состав которых входят соответствующие множества $Z_1 = \left\{ z_{1r}, r = \overline{1,m} \right\}$, $Z_2 = \left\{ z_{2r}, r = \overline{1,m} \right\}$ и существует функциональное преобразование f,

с помощью которого отображения γ_1 можно взаимно однозначно перевести в отображение γ_2 ($\gamma_2 = \gamma_1 f, \gamma_1 = \gamma_2 f^{-1}$), то шкалы $\langle S, C_1, \gamma_1 \rangle$ і $\langle S, C_2, \gamma_2 \rangle$ считаются принадлежащими к одному типу, а преобразования *f* называется допустимым преобразованием.

Введение понятия допустимых преобразований несколько трансформирует принятое в рамках классического подхода [43] определение понятия шкалы как тройки $\langle S, C, \gamma \rangle$. Согласно современным представлениям, наиболее полной и содержательной характеристикой шкалы есть множество *Ф* допустимых преобразований значений эмпирической свойства, измеренных в данной шкале. В зависимости от состава множества *Ф*, характерного для определенных типов шкал, возможно проведение структуризации множества произвольных шкал, результатом которой является построение типологии шкал. Общепринятый вариант такой типологии приведен в табл. 3.2.

Таблица 3.2. Типология множества произвольных шкал

Тип шкалы	**Допустимые преобразования для данного типа шкалы**
Номинативная	Взаимно-однозначные: $(x_1 = x_2) \equiv (f(x_1) = f(x_2))$
Порядковая	Монотонно возрастающие: $(x_1 < x_2) \equiv (f(x_1) < f(x_2))$
Интервальная	Положительные линейные: $f(x) = ax + b;$ a, b – произвольные действительные числа, $a > 0$
Шкала отношений	Преобразование подобия: $f(x) = ax, \quad a > 0$
Абсолютная	Тождество: $f(x) = x$

При анализе введенной типологии, в частности, сравнении различных типов шкал, обычно используются понятия сильных (мощных) шкал и, соответственно, слабых. Назовем одну из двух шкал более сильной (мощной), если множество ее допустимых преобразований среди других включает все допустимые преобразования, присущие второй шкале.

Наиболее слабым типом шкалы считается **номинативная** (иначе – шкала наименований). В ней числа являются лишь условными наименованиями классов, на которые разделено исходное множество объектов, то есть выполнение математических операций с

этими числами некорректно, числа играют роли имен. Например: предоставление множеству женщин условного числового обозначения «α», множеству мужчин – «β», в частности α=1, β=2, или любые другие числовые обозначения.

Более сильной есть **шкала порядка** (порядковая, ординальная), в которой все объекты строятся по определенному признаку (свойству): по принципу его роста (увеличения) или наоборот, то есть для объектов, которые сравниваются с эмпирическим свойством *X*, должно устанавливаться отношение порядка: $x_1 < x_2 \le x_3 <...< x_n$. Существенно то, что принцип пропорциональности в этой шкале не выполняется, то есть нельзя указать, насколько x_2 лучше x_1 (в общем случае – x_i лучше, чем x_j, если $j<i$).

Шкала интервалов является частично метрической, позволяет применять линейные преобразования, но не имеет установленной точки нулевого отсчета, точнее, эта точка может устанавливаться произвольно.

Еще более сильной является **шкала отношений** (пропорциональная). Это метрическая шкала, в которой допустимо изменение масштаба и которая имеет «естественную» нулевую точку. Это типичная шкала для измерения большинства технических или физических величин (скорости, веса, емкости), денежных состояний и т.д.

Абсолютная шкала является наиболее мощной (сильной) шкалой. Для нее множество допустимых преобразований содержит тождественное преобразование $f(x)=x$, то есть фактически полученный результат измерений является единственно возможным и в отношении него недопустимы любые дополнительные преобразования. Абсолютная шкала метрическая, имеет естественную нулевую точку отсчета и естественную единицу измерения – единицу счета. Эта шкала удобна для измерения количества элементов в конечном множество, то есть является шкалой натуральных чисел. Физический пример абсолютной шкалы – шкала температур по Кельвину.

Приведенные в табл. 3.1 типы шкал образуют своеобразную иерархию, в которой каждая последующая шкала включает в себя предыдущую и поэтому является более мощной по сравнению со

всеми предыдущими. Таким образом, абсолютная шкала будет иметь свойства всех других, то есть из данных, полученных в абсолютной шкале, можно определить все, что могут дать измерения в других шкалах.

Например, если известно, что в группе А – 20 студентов, а в группе В – 10 студентов, то верны следующие выводы: в группе В студентов вдвое меньше (шкала отношений), их меньше на 10 (шкала интервалов), группа А количественно больше группы В (порядковая шкала), количество студентов в группах неодинаково (номинативная шкала).

Следует отметить, что в типологии выделены только основные типы шкал. Поэтому нужно принять во внимание, что каждый отдельный тип шкалы может иметь многочисленные модификации, а пара основных типов способна породить множество промежуточных, смешанных (или комбинированных) шкал. Кроме того, для современного понимания шкалы совсем не обязательно отражать ЕСО в ЧСО – вместо последнего может быть другая формальные знаковая система, с помощью которой можно адекватно смоделировать ЕСО.

Экспертно-аналитическая процедура оценивания значимости информационных ресурсов в общем случае

Рассмотрим следующую ситуацию. Существует совокупный (множественный) ИР J_{Σ}, содержащий информацию о разнообразнейших отраслях человеческой деятельности, который постоянно пополняется, расширяется, но при этом предполагает возможной свою фрагментацию на частичные ИР. Уровень этой фрагментации может быть произвольным, в зависимости от требуемой степени детализации описаний объектов (элементов) в той или иной предметно-прикладной области деятельности. Степень детализации может меняться со временем, поэтому фрагментация исходного ресурса J_{Σ} на частичные носит динамический характер. Нужно построить процедуру оценивания ценности (значимости) выделенных частных ИР.

Очевидно с течением времени объем обобщенного ресурса J_{Σ} будет увеличиваться, что является естественным следствием циви-

лизационного процесса. Совокупная значимость ресурса J_{Σ} будет, по-видимому, расти. Закономерности изменения ценности (значимости) частичных ИР, которые зависят от влияния множества самых разнообразных и, как правило, лишь частично учтенных факторов, практически не поддаются прогнозу и могут проявляться самым неожиданным образом. Поэтому единственным способом определения значимости частичных ИР является экспертная оценка, ошибки которой носят субъективный характер и зависят только от уровня компетентности экспертов и сложности поставленной перед ними задачи. Подбор компетентных экспертов является организационным моментом подготовки экспертизы и рассматривается отдельно (Глава 4).

В связи с этим остановимся лишь на минимизации ошибки, обусловленной сложностью объекта экспертизы. Один из вариантов решения этой задачи заключается в отказе от проведения традиционной одноэтапной экспертизы с нахождением прямых оценок значимости ИР и переходе к экспертно-аналитической процедуре формирования оценок, которая, в отличие от обычной экспертизы, использует поэтапное структурирование процесса экспертизы и определенную логическую регламентацию содержания его отдельных этапов.

При формировании экспертно-аналитической процедуры оценивания ценности (значимости) ИР учитывается два принципиальных аспекта, а именно:

− сужение предметной области объектов экспертизы, образованной совокупностью ИР, относительно ценности, которых должен определиться эксперт, что позволяет упростить подбор экспертов с высоким уровнем компетентности;

− учета возможного наличия к моменту проведения экспертизы ИР определенного количества уже оцененных ресурсов, что существенно упрощает принятие решения о новом, еще не экспертированом ИР, и делает целесообразным выделение двух не совпадающим типовых задач определения ценности ИР [32]:

1) задачи первичной экспертизы ИР, где оценке подлежит вся исходная совокупность ИР, составляющих совокупный (множественный) информационный ресурс J_{Σ};

2) задачи вторичной экспертизы, где часть частных ИР уже прошла первичную экспертизу.

Возможны различные способы построения экспертно-аналитической процедуры, которые зависят от объектов экспертизы и сформированных в соответствующих предметных областях традиционных подходов к проведению экспертизы. В частности, опираясь на приведенные в [32] материалы для выполнения первичного экспертно-аналитического оценивания значимости ИР можно предложить следующую последовательность действий.

1. Весь представленный к экспертизе совокупный ресурс J_Σ представляется в виде объединения ресурсных областей J_i, которые не пересекаются, и каждая из которых соответствует определенной предметно-прикладной сфере:

$$J_\Sigma = \bigcup_{i=1}^{n} J_i \ , \ i = \overline{1,n} \ , \ J_i \cap J_j = \emptyset \text{ при } i \neq j.$$

2. В каждой отдельной ресурсной области J_i выделяются группы ресурсов, допускающих по своим характеристикам и уровнями значимости взаимное сопоставление. Задаются приближенные (грубые) границы диапазонов оценок соответствующих ресурсных групп, среди которых выбирается самый верхний $C_{max\ i}$ и самый нижний $C_{min\ i}$ пределы, определяющие верхнюю и нижнюю границы шкалы оценок для соответствующей предметно-прикладного сферы. Полученные пары ($C_{max\ i}$, $C_{min\ i}$), $i = \overline{1,n}$ оцениваются в условных единицах (баллах), которые не привязаны к какой-либо конкретной денежной единицы. Сопоставление этих пар, определенных для различных предметно-прикладных отраслей, позволяет осуществить согласование и увязку уровней значимости информации по всему множеству ИР, которые входят в совокупный ресурс J_Σ, а также вносить необходимые текущие коррекции в случае естественной смены значимости ИР отдельных предметно-прикладных отраслей. При этом становится очевидной определенная конвенциональность полученных оценок значимости информации, которые зависят, в частности, от полноты и репрезентативности системы частных ИР, составляющих совокупный ИР J_Σ.

3. Для множества частных ИР $\{I_{kl}\}$, $l=\overline{1,L_k}$, образующих *k*-ю ресурсную группу I_k, экспертным путем с помощью метода парных сравнений выполняется упорядочение исходной совокупности соответствующих частных ИР.

В рамках этой классификационной процедуры для элементов, сопоставляющихся в ресурсной группе I_k, путем введения бинарного отношения $\leq$ на множестве частных ИР $\{I_{kl}\}$, $l=\overline{1,L_k}$, формируется решетка ценностей *ИР* этой ресурсной группы.

4. Для упорядоченной совокупности частных ИР определяется множество их оценок значимости $\{c_{kl}\}$.

Применяя метод экспертных оценок, каждому элементу сформированной решетки приписывается количественное значение его ценности, совокупность которых образует искомое множество оценок значимости $\{c_{kl}\}$ соответствующих частных ИР. При оценивании значимости с применением векторных критериев, то есть когда значимость ИР определяется рядом потребительски важных признаков, для нахождения результирующих оценок значимости целесообразно применять известные методы многокритериального анализа, в частности метод анализа иерархий (МАИ) [36].

После нахождения множеств оценок значимости частных IP для отдельных ресурсных групп получим множество ИР всей ресурсной области J_i, а затем – всего совокупного ресурса J_Σ. В случае необходимости возможно проведение дополнительных экспертиз с целью проверки качества полученных оценок ценности через попарное сопоставление базовых элементов отдельных ресурсных групп и областей и приписанных им количественных оценок ценности. После этого задачу первичной экспертизы ИР можно считать выполненной.

Если выполнение работ осуществляется группой экспертов в соответствии с содержанием этапов пп. 1-4, для обработки полученных в этом случае результатов целесообразно использовать методы теории нечетких множеств [44].

Задачу вторичной экспертизы рассмотрим на примере экспертизы нового единичного частного ИР (очевидно, вторичная эксперти-

за группы новых частных ИР может быть просто сведена к этому примеру).

При появлении нового частного ИР прежде всего определяется конкретная предметно-прикладная сфера, к которой принадлежит этот новый ИР, то есть соответствующая этому ИР ресурсная область и ресурсная группа. Далее эксперт, компетентный в этой сфере, сначала обнаруживает местоположение нового ИР в линейно упорядоченном множестве частных ИР, которые образуют решетку ценностей (например, применив метод парных сравнений), а затем, завершая экспертизу, количественно оценивает ценность (значимость) нового частного ИР, используя, если в этом есть необходимость, МАИ. При этом количество элементов решетки увеличивается на единицу, а классификация очередного следующего нового ИР происходит в более детализированной решетке.

Если появление нового частного ИР требует переформатирования ранее существовавших (в частности, объединение уже существующих ресурсных групп или наоборот, их детализацию и разделение на более мелкие), необходимо сопоставить его с близкими информационными комплексами, полученными на предшествующих (более ранних) фрагментациях совокупного ресурса J_{Σ}, сравнить их объемы и содержание, проверить возможность наличия включений одного ресурса в другие. Это позволит в определенной степени упростить процедуру определения ценности (значимости) нового ИР и ввести в нее элементы контроля.

При увеличении объема ИР за счет объединения некоторых частных ресурсов следует учитывать возможность скачкообразного роста уровня ценности нового интегрированного ИР вследствие возможного проявления в нем эффекта эмерджентности [24-26].

В общем процедуру определения ценности (значимости) некоторого частичного ИР можно интерпретировать как измерение ценности этого ресурса в сложной комбинированной шкале, формирование которой выполнено в соответствии с пп. 1-3.

Рассмотрим состав и структуру этой шкалы. Распределение совокупного ресурса J_{Σ} по предметно-прикладным сферам фактически представляет собой построение номинативной шкалы, которая обеспечивает грубую предварительную классификацию множества

возможных частных ИР. Внутри каждой номинации (класса той шкалы, которому соответствует ресурсная область J_i, $i=\overline{1,n}$) осуществляется более детальная классификация частных ИР по ресурсным группам. В результате получаем набор локализованных номинативных шкал, по одной на каждую ресурсную область. В целом эта структура представляет собой двойную иерархическую номинативную шкалу. Если количество частных ИР, входящих в некоторые номинации второго уровня иерархии, велико, для этих номинаций целесообразно сформировать еще один, третий уровень номинативной шкалы. Очевидно, что при необходимости можно наращивать еще более высокие уровни шкалы. В номинациях последнего уровня, в нашем случае, согласно п.3 – второго уровня номинативной иерархии, множество частных ресурсов в пределах каждой ресурсной группы I_k упорядочивается по своей значимости, образуя порядковую шкалу вида: $I_{k(1)} \le I_{k(2)} \le ... \le I_{k(l)} \le ... I_{k(L)}$, которая является шкалой третьего уровня иерархии.

Учитывая, что каждой ресурсной группе I_k ставится в соответствие некоторый диапазон оценок в баллах ($c_{k\ max}$, $c_{k\ min}$], получаем комбинированную построчно-интервальную шкалу. Приписывая каждому элементу I_{kl} экспертную оценку в баллах c_{kl}, $k=\overline{1,L}$, усиливаем порядковую шкалу до интервальной. Это усиление носит искусственный характер, правильность полученных результатов определяется исключительно точностью соответствующих экспертных оценок c_{kl}. Следует отметить, что неявная попытка усиления шкалы присутствует и на этапе построения двойной иерархической номинативной шкалы, при введении балльных значений границ диапазонов оценок ($c_{k\ max}$, $c_{k\ min}$], $k=\overline{1,L}$ ресурсных границ, что делает возможным метризацию порядковых шкал для ресурсных групп.

Введение подобной комбинированной измерительной шкалы позволяет относительно легко реализовать оценивания уровня значимости некоторого ИР I', интерпретировав процедуру оценивания как решение обобщенной задачи измерения в этой шкале. В частности, используя двойную иерархическую номинативную шка-

лу, достаточно просто найти ресурсную группу, к которой относится ресурс I', а потом экспертным или экспертно-аналитическим путем определить положение ресурса I' в соответствующей локальной порядковой шкале и количественную оценку уровня значимости этого ИР.

Проиллюстрируем возможность применения современной теории измерений к задачам оценивания уровня потерь, обусловленных утечкой СИ. При этом будем опирается на применение двух базовых методов прикладного анализа информации: метода парных сравнений и нониусного подхода к классификации информации.

Классический метод парных сравнений позволяет расположить элементы, составляющие некоторое множество, в порядке увеличения или уменьшения признака, общего для всех элементов данного множества. Известна также методика, когда подобная классификация (ранжирование) происходит по нескольким признакам (по комплексу или по вектору признаков), – МАИ [36]. К сожалению, парные сравнения хорошо работают в условиях, когда количество анализируемых элементов множества невелико. С увеличением объема этого множества трудоемкость и сложность применения метода парных сравнений резко возрастает, что в данной ситуации делает его непригодным для практического использования.

Выходом в этом случае может быть своеобразный гипертекстовый вариант сравнительного анализа, в котором исходная совокупность элементов делится на определенные подмножества, образующие уже рассмотренную выше так называемую нониусную линейку шкал. Эта линейка является своеобразной иерархией шкал, каждая из которых, начиная со второй, соответствует более точной вспомогательной нониусной шкале, которая детализирует, уточняет отдельные элементы (фрагменты) предыдущей грубой шкалы более высокого уровня нониусной иерархии.

Например, первую – грубую шкалу (высокий уровень иерархии) образуем четверкой информационных блоков, содержащих информацию в сферах:

1) обороны;
2) экономики, науки, техники;
3) внешних отношений;
4) государственной безопасности и охраны правопорядка.

Каждый из перечисленных блоков грубой номинативной шкалы может быть представлен более детализировано подмножеством конкретизирующих его содержание вспомогательных информационных элементов, например:

3.1) общие сведения о дипломатических отношениях с другими государствами;

3.2) сведения о договоренностях в сфере военно-технического сотрудничества с иностранными государствами;

3.3) ..... .

Эти информационные элементы предполагают ранжирование по уровню потерь, обусловленных утечкой соответствующей информации, то есть образуют нониусную ранжированную шкалу второго уровня. При необходимости возможна конкретизация отдельных (или всех) элементов этой шкалы введением дополнительных множеств детализирующих информационных элементов. Например, п. 3.2) может получить расширение:

3.2.1) информация о международных соглашениях в области разработки вооружений и военной техники;

3.2.2) информация о международных контрактах в сфере поставок вооружений и военной техники;

3.2.3) ..... .

Дополнительно введенные информационные элементы после их ранжирования по уровню возможных потерь вследствие утечки соответствующей информации образуют нониусную ранжированную шкалу третьего уровня. Продолжая, если это целесообразно, процедуру детализации информационных элементов шкалы третьего уровня, получим нониусные ранжированые шкалы еще более высоких уровней.

В конце концов, в результате применения подобного нониусные подхода к классификации секретной информации получаем структура представления информации, подобную структуре ССГТ.

Упорядоченное таким образом множество информационных элементов образует систему номинативно-ранговых шкал, в которую эксперт имеет возможность «встроить» любой новый элемент, для которого необходимо оценить уровень возможных потерь из-за разглашения содержания данного элемента. Для этого эксперт определяет на нониусной линейке шкалу, ближайшую по содержа-

нию и уровню детализации к объекту оценивания и выполняет ряд парных сравнений объекта с узлами (элементами) выбранной шкалы. Место, которое занял объект оценивания в системе ранговых шкал, можно в дальнейшем воспринимать как новый узел шкалы, что в дальнейшем будет использован в процедуре следующих парных сравнений при оценке новых информационных элементов.

Для определения принадлежности оцениваемой информации к секретной необходимо получение количественных оценок возможных потерь, обусловленных разглашением этой информации, которые в порядковой (ранжированной) шкале рассчитать нет возможности. Поэтому следует выполнить метризации нониусной системы шкал, присвоив ее узлам-элементам количественные оценки уровней потерь.

Для этого рассматривается все, что имеет определенную ценность (имиджевую, экономическую, политическую и т.д.) и в той или иной степени может быть ассоциировано с соответствующим информационным элементом. В ДСТУ ISO/IEC 13335 [30] это «все» определяется термином «активы», связанные с информационным элементом, а убытки, обусловленные уменьшением ценности активов вследствие утечки информации, выступают в качестве количественной оценки уровня соответствующих потерь.

В Методических рекомендациях государственным экспертам по вопросам определения оснований для отнесения сведений к государственной тайне и степени их секретности (далее – Методические рекомендации) [45] эти активы (в очень сокращенном объеме) приведены в Приложении (см. *Приложение 5*), где их ценность определяется термином «удельный вес» объекта той или иной сферы деятельности (обороны, экономики, государственной безопасности и т.д.). Очевидно, что эффективное применение подобной методики оценки потерь возможно лишь при условии очень подробных перечней активов в каждой сфере деятельности, связанной с использованием секретной информации, в частности, при составлении таких списков для каждой шкалы нониусной линейки шкал.

Кроме того, следует иметь в виду, что потери информации только по содержанию одного информационного элемента могут обусловить убытки по различным активам, то есть следует анализиро-

вать и рассматривать различные варианты событий, толчком к которым стала потеря соответствующей информации.

В развернутой постановке задача шкалирования и измерения ценности информации, включая некоторые сведения из теории обобщенного измерения, построения и интерпретации систем нониусных (комбинированных) шкал (в том числе и для Методических рекомендаций [45]), рассмотрена в статье [15]. Интересно сопоставление предложенных теоретических рекомендаций и выводов с положениями Методических рекомендаций, в основу которых положен многолетний опыт, наработанный в течение длительной работы государственных экспертов по вопросам гостайны. Учитывая это замечание, в двух следующих разделах будут рассмотрены некоторые практические аспекты анализа потерь, обусловленных потерей СИ.

Интерпретация содержания базовых положений Методических рекомендаций [45] с позиций современной теории измерения и применения системы комбинированных шкал

Вопрос выбора шкалы измерения обычно обуславливается двумя требованиями.

Первое – это соответствие характера отношений в ЕСО типу шкалы. Дело в том, что мощность шкалы ограничена сверху видом существующих в ЕСО отношений. Например, если измеряемая свойство предполагает только отношение порядка, невозможно количественное измерение уровня этого свойства, следовательно, исключается применение количественных (метрических) шкал – интервальной и отношений, возможен выбор – номинативная или порядковая шкала. Из этих двух шкал более сильная порядковая, и именно она адекватна характеру отношений в ЕСО. Применения более слабой номинативной шкалы обусловит неполное использование информации, которую несут в себе отношение порядка, а потеря информации вследствие упрощения шкалы (из порядковой в номинативную) ведет к примитивизации процедур обработки результатов измерения, в частности к уменьшению допустимых методов обработки данных, упрощению алгоритмов обработки и т.д.

Второе требование – соответствие шкалы определенной цели, достижению которой подчиняется сама необходимость измерения.

Чаще всего это – построение математической зависимости, в которую входит измеряемая свойство, множество допустимых операций, использующих полученные результаты измерения, теоретические, эвристические, аппроксимативные модели, в которые измеряемое свойство привлекается в качестве переменной. В подобных ситуациях обычно возникает потребность в использовании метрических (количественных) шкал, применение которых обеспечивает возможность выполнения над полученными результатами измерений широкого спектра операций математической обработки данных.

Интересно проанализировать учета двух указанных выше требований в Методических рекомендациях государственным экспертам по вопросам определения оснований для отнесения сведений к государственной тайне и степени их секретности. В частности, исследования, приведенных в Методических рекомендациях [45] базовых соотношений по определению уровня совокупного вреда W (балльное значение которого является главным фактором в принятии решения о принадлежности сведений к государственной тайне (ГТ)) позволяет сделать ряд важных выводов.

Согласно Методическим рекомендациям, совокупный ущерб W сочетает две составляющие: $W = W_{ек} + W_{пр}$, которые, в соответствии с характером отношений в исходных ЕСО, должны измеряться в разных шкалах [15, 16].

Составляющая $W_{ек}$ – показатель экономического ущерба, который означает уровень снижения эффективности использования выделенных средств для обеспечения деятельности объекта вследствие разглашения сведений об этом объекте. Учитывая наличие естественной нулевой отметки (в случае $W_{ек} = 0$ информация, проверяемая на принадлежность к секретной, таковой на самом деле не является), составляющая $W_{ек}$ предполагает применение метрических шкал, в частности, шкалы отношений.

Составляющая $W_{пр}$ – показатель, характеризующий ущерб государству от других тяжелых последствий, которые не могут быть просчитаны в количественном или стоимостном выражении. Поэтому оценки значений составляющей $W_{пр}$ реализуется исключи-

тельно экспертным путем, и полученные таким образом результаты имеют качественный характер, то есть им соответствует номинативная или порядковая шкала.

Учитывая, что совокупный ущерб W образуется из составляющих $W_{ек}$, $W_{пр}$ операцией сложения, которая требует представления обоих составляющих в количественной шкале, возникает потребность в повышении мощности шкалы измерения составляющей $W_{пр}$. Для системы соотношений, по которым путем сопоставления значения W с набором пороговых значений {1, 10, 100} определяется степень секретности, достаточной будет шкала интервалов. Однако эта шкала должна иметь определенные особенности, в частности, фиксированную нулевую отметку $W = 0$ и искусственно введенную единицу измерений, общую для $W_{ек}$, $W_{пр}$, W. Очевидно, что данная шкала должна быть одинаковой для всех трех вышеупомянутых переменных, то есть требуется проведение определенных мер по взаимосвязи выходных типов шкал, составляющих $W_{ек}$, $W_{пр}$. Чтобы удовлетворить эти требования, оставаясь в рамках перечня эмпирико-эвристических правил, приведенных в Методических рекомендациях, можно предложить следующие механизмы преобразования шкал [15, 16].

Сначала рассмотрим повышение мощности шкалы для измерений $W_{пр}$, которое выполним в четыре этапа.

1. Введем конечное множество из π тяжелых последствий, которые являются элементами номинативной шкалы и каждому из которых в соответствие поставлена достаточно полная спецификация.

2. На базе введенного множества тяжелых последствий построим порядковую шкалу, определив в ней L классов:

класс C_1 − последствия первой категории (подмножество π_1),

класс C_2 − последствия второй категории (подмножество π_2),

…

класс C_L − последствия L-й категории (подмножество π_L),

где $\bigcup_{k=1}^{L}\pi_k = \pi$; $\pi_k \cap \pi_r = 0$ для $k, r = \overline{1, L}$, $k \neq r$.

3. В пределах каждого класса порядковой шкалы из элементов соответствующего подмножества создадим частную номинативную шкалу.

4. Каждому классу порядковой шкалы сопоставим соответствующий полуоткрытый интервал балльных оценок: $C_1 - (w_1, \infty)$ баллов, $C_2 - (w_2, w_1]$ баллов, …, $C_k - (w_k, w_{k-1}]$ баллов, …, $C_L - (w_L, w_{L-1}]$ баллов.

Благодаря реализации последнего этапа путем экспертного оценивания можем получить уточненные балльные оценки для конкретных элементов частичных номинативных шкал. В целом полученная шкала представляет собой комбинированную порядково-номинативную шкалу, искусственно усиленную до интервальной, которая позволяет дать приблизительные количественные оценки возможных других тяжелых последствий, обусловленных разглашением секретных сведений.

Процедура оценивания уровней вреда $W_{пр}$, которые являются следствием развертывания определенного сценария событий, связанных с разглашением секретных сведений, в такой комбинированной шкале осуществляется следующим образом.

Сначала, анализируя состав элементов подмножеств π_k, $k = \overline{1, L}$ частных номинативных шкал, следует определить (хотя бы очень приближенно), к какому из классов порядковой шкалы тяжелых последствий можно отнести последствия реализации рассматриваемого конкретного сценария событий. Если предположить, что это класс C_k, то дальше, опираясь на принадлежащий данном *k*-ом классу C_k диапазон балльных оценок $(w_k, w_{k-1}]$, дать экспертную оценку уровню потерь $W_{пр}$, обусловленному реализацией соответствующего сценария.

Если в описанной выше порялково-номинативной шкале положить количество классов L=5 и ввести множество

$\{w_1, w_2, w_3, w_4, w_5\} = \{200, 100, 70, 50, 10\}$, то получим приведенный в Методических рекомендациях Перечень важных иных тяжелых последствий для интересов государства от разглашения секретных сведений (далее - Перечень). То есть Перечень – это частная шкала, по которой эксперты должны определять количественные значения показателя $W_{пр}$. Следует заметить, что введенный в Методических рекомендациях Перечень не имеет научно-методологического обоснования и, очевидно, носит исключительно эмпирико-эвристический характер. Предложенная выше порядково-номинативная шкала опирается на базовые положения общей теории измерения, что позволяет обосновать способ ее построения, объяснить структуру этой шкалы, сформировать процедуру определения оценок $W_{пр}$, оценить их корректность (уровень доверия к полученным количественных значений) и в случае необходимости целенаправленно и осмысленно трансформировать эту шкалу, обеспечивая ее оптимизацию, адаптацию или совершенствование.

К сожалению, точность полученных значений $W_{пр}$ существенно зависит от полноты и достаточности множества π возможных тяжелых последствий. В связи с этим следует отметить, что определенный в [45] Перечень является весьма узким и требует неотложного развития с желаемой дифференциацией по четырем сферам деятельности, определенным статьей 8 закона Украины «О государственной тайне». Упомянутое распределение сфер деятельности обостряет ситуацию с решением и другой сформулированной выше задачи – согласованием шкал показателей $W_{пр}$, $W_{ек}$. Шкала $W_{ек}$, как это уже было выяснено, – это шкала отношений, поэтому оценки, полученные в ней (в том числе в различных сферах деятельности), не имеют естественной совместной масштабной единицы, и «вес» баллов в различных сферах деятельности может не совпадать. В Методических рекомендациях для практического решения этой проблемы предлагается применение сведенных в таблицу так называемых «удельных весов» важных объектов (далее в тексте – Таблица). Введение этой Таблицы, как и введение рассмотренного

выше Перечня, ничем не обосновывается, то есть опять же существуют рекомендации только эвристического характера.

Фактически Таблица представляет собой двойную иерархическую номинативную шкалу. Верхний уровень иерархии состоит из трех номинативных классов:

1. Оборона.
2. Экономика.
3. Государственная безопасность.

Нижний уровень образуется внутренними (отраслевыми) номинативными шкалами, с элементами которых соотнесены определенные балльные оценки. Они и определяют «удельный вес» соответствующего элемента (объекта, содержащего сведения, которые подлежат экспертизе). То есть на нижнем уровне есть комбинированные шкалы, номинативные по структуре, однако с количественными характеристиками номинантов. Последнее, в зависимости от опыта и уровня знаний эксперта, позволяет ему путем сравнительного анализа определить балльные оценки конкретных объектов, непосредственно отсутствующих в Таблице. Это происходит путем их прямого сопоставления с ближайшими номинантами, т.е. фактически работает ниусный метод оценивания. Еще одним возможным способом оценки объектов является детализация содержания или структуры номинантов путем декомпозиции их на составляющие элементы с последующим распределением оценки каждого из номинантов на соответствующей совокупности его составляющих. Полученное таким образом множество оценок позволяет установить ценность менее весомых объектов оценивания, а затем использовать их в расчетах балльных оценок новых сложных (составных) объектов путем суммирования оценок составляющих, входящих в состав соответствующего нового объекта. Совокупность ряда детализирующих элементов можно рассматривать как новый третий уровень номинативной иерархии, то есть такая иерархическая структура шкалы предполагает саморазвитие, целью и результатом которого является детализация шкалы. Очевидно, что в общем случае возможно развитие и уже существующих шкал, в частности шкал верхнего уровня за счет включения в них новых номинативных классов.

Возможность саморазвития иерархических шкал снимает одно из важнейших замечаний в адрес таблицы «удельных весов» – ограниченность множества объектов, введенных в Таблицу, и ее недостаточную детализацию. В определенной степени примером детализации Таблицы можно считать Свод сведений, составляющих государственную тайну [23].

В случае необходимости саморазвитие возможно и для ранее рассмотренной шкалы перечня «удельных весов». Отличие этой шкалы заключается в том, что ее второй уровень образуют частные порядковые шкалы. Поэтому детализация такой шкалы ведет к увеличению числа элементов в пределах каждой из порядковых шкал без введения дополнительных уровней. Фактически это своеобразное интерполяционное наполнения порядковых шкал путем включения новых элементов между смежными, введенными ранее. Важно, что этот процесс способствует формированию естественной интервальной шкалы. Следует отметить, что, исходя из анализа существующего математического инструментария для подобной «интерполяции» с успехом можно применить аппарат нечетких множеств.

Приведенное выше в первую очередь ориентировано на изложение формальных аспектов разработки шкалы измерения вреда, обусловленного разглашением информации. Практическая сторона оценки уровня этого ущерба имеет свои особенности. Прежде всего это нестабильность полученных оценок во времени, связанная с постоянными изменениями, нестабильностью связей и отношений социальной, экономической, политической и других сфер цивилизационного процесса, поскольку именно этот процесс является единственной формой существования социума.

Следствием этого является компромиссный характер указанного выше стремление к детализации шкалы: с повышением уровня детализации оценки ущерба на нижних уровнях шкалы становятся все более вариабельными, динамическими, что иногда делает целесообразным переход к более грубой (менее мощной) шкале, для которой колебания количественных значений оценок являются не столь существенными. То есть детализация низшего уровня комбинированных шкал может привести к потерям мощности шкалы на этом уровне. Как пример, можно рассматривать ССГТ: по своей

структуре он фактически представляет собой шкалу, близкую к шкале «удельных весов», однако, во-первых, значительно более детальную, во-вторых, на более низком уровне представленную в шкале рангов (секретно, совершенно секретно, особой важности). Ранжированные оценки гораздо менее чувствительны к колебаниям ситуативного характера в сферах деятельности, по которым структурировано ССГТ.

Еще одним важным аспектом практического построения шкал является согласование между собой количественных оценок (как «удельных весов», так и иных тяжелых последствий), которые применяются для определения ущерба в различных сферах деятельности. Данные об оценках, приведенные в Методических рекомендациях, считаются «не вызывающими сомнений», что считается само собой очевидным, ибо они установлены экспертами, уровень компетенции которых является самым высоким. Тем не менее в общем случае это должно быть подтверждено результатами определенных проверок.

Например, в отдельных случаях возможно получение количественных оценок в реальном денежном выражении. Наличие таких реальных денежных оценок в различных сферах деятельности позволяет, сопоставив их балльные оценки, сбалансировать значения всех других балльных оценок. Однако практическое решение этих вопросов требует прежде всего очень высокого уровня компетентности экспертов в соответствующих сферах.

3.5. Сценарный метод оценивания ущерба, причиненного утечкой секретной информации

Уровень вреда, обусловленного разглашения секретной информации, является, следствием действий стороны, которая завладела этой информацией. При этом предполагается многовариантность возможных действий стороны, причем в общем случае эти варианты разновероятны. Традиционное сведение множества вариантов к одному наиболее вероятному для систем, относящихся к классу сложных (а это прежде всего социальные и социотехнические системы) не является приемлемым, так как имеет очевидно субъективный характер и, кроме того, может существенно снизить оценку

ущерба из-за не учёта других, менее вероятных, но более тяжелых последствий.

Таким образом, оценка окончательного вреда, обусловленного утечкой секретной информации, должна базироваться на учете частных оценок ущерба, полученных по различным вариантам развития событий, каждый из которых является следствием возможных действий стороны, завладевшей секретной информацией. То есть фактически сталкиваемся с задачей прогнозирования событий в сложной социальной системе, зависящих от конкретной ситуации в политической, экономической, социотехнической и других сферах.

Социальное прогнозирование – достаточно сложный процесс, для которого точность полученного решения зависит от множества факторов, в частности использования и соблюдения требований научно обоснованных методик генерации и отбора вариантов развития прогнозируемой ситуации. При этом, как отмечалось в [46], в данном случае наибольшую актуальность приобретает вопрос выбора способов и средств многовариантного прогноза. Некоторой риторичности этому вопросу придает общее признание эффективности применения в таких задачах метода сценариев [47, 48], либо как его называют в ряде работ [49-51] – сценарного подхода или сценарного анализа.

Существенная особенность сценарного подхода заключается в том, что он, в отличие от классических методов математического прогноза, не дает количественной оценки будущего значения определенного прогнозируемого параметра или группы параметров, а формирует множество возможных состояний, к которым может развиться исходная ситуация под влиянием тех или иных факторов. Это позволяет утверждать, что сценарный подход можно рассматривать как специфический вид социального планирования. По выражению Э. Янга, «сценарий не предсказывает будущее, а формирует его варианты при наличии соответствующих предпосылок» [52], то есть под сценарием обычно понимают описание возможного развития событий в определенной ситуации.

Суть и схему применения сценарного подхода можно объяснить на примере анализа функционирования определенного социального объекта, процесс устойчивой и предсказуемой жизнедеятельности

которого прервался появлением аномалии – возникновением чрезвычайной (критической) ситуации [16]. Для прогнозирования характера дальнейшего функционирования исследуемого объекта генерируются (строятся) так называемые сценарии – модели возможных в будущем вариантов развития событий. Отправной, начальной точкой для всех сценариев является момент возникновения критической ситуации, однако последующее развитие событий по каждому из сценариев имеет свои индивидуальные особенности и различия, а конечные события и последствия реализации каждого из сценариев могут быть совершенно разными. Обычно целью сценарного прогнозирования является анализ и изучение состава и последовательности событий каждого из сценариев, анализ причинно-следственных связей между событиями и определение вероятностей реализаций соответствующих сценариев вместе с оценкой конечного состояния исследуемого объекта после завершения каждого из сценариев. Результатом выполнения такого сценарного анализа чаще всего является принятие определенного решения и соответствующих управленческих действий, которые позволяют в определенном смысле оптимизировать процесс вывода социального объекта из сложившейся чрезвычайной (критической) ситуации. В еще более общей постановке методология сценарного анализа должна обеспечить прогноз и выявление возможного появления аномальности в процессе функционирования социального объекта, то есть развития любых чрезвычайных ситуаций, альтернативных состоянию его нормального функционирования.

Формально сценарий S можно описать, задав:

а) декомпозицию сценария на совокупность последовательных событий-сцен, где каждая предыдущая сцена s_l трансформируется ($\rightarrow$) в следующую s_{l+1}:

$$\{s_k\} = \{s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow ... \rightarrow s_k\};$$

б) завершения каждого события s_l характеризуется определенным состоянием X_l / s_l исследуемого объекта:

$$X_l / s_l = [(x_{l1}, x_{l2}, ..., x_{lm},) / s_l], \ \ l = \overline{1,k},$$

где $x_i, i = \overline{1,m}$ – переменные, описывающие функционирование объекта во времени;

в) вероятность p реализации сценария S и последствия q этой реализации, в частности q может означать определенные потери, которые понес объект после выхода из чрезвычайной ситуации по сценарию S.

В общем, описание сценария S может быть задано четверкой $<\{s_k\}, \{X_k / s_k\}, p, q>$.

Если есть несколько сценариев $s_1, s_2, ..., s_n$, которые по условиям своей реализации образуют полную группу, то, если q по своей сути является характеристикой потерь, можем определить вероятные потери Q после выхода объекта из чрезвычайной ситуации как средний риск:

$$Q = \sum_{i=1}^{n} p_i q_i,$$

где $p_i q_i$ – частный риск реализации i-ого сценария.

Считается, что впервые метод сценариев применил Герман Кан для исследования сложных систем [53]. Сначала сценарии носили чисто описательный характер, затем стали использоваться более формализованные конструкции [51]. Существуют различные концепции генерации сценариев, однако завершенного решения данной проблемы сегодня нет.

На практике для генерации сценариев используется достаточно широкий спектр методов, существенно отличающихся по условиям и особенностям своего применения [47, 48, 50, 51]. Среди формализованных методов, позволяющих в определенной степени упорядочить процесс анализа критической (проблемной) ситуации и создать объективные условия для построения множества реалистичных вариантов (альтернатив) сценариев, можно в качестве примера привести метод морфологического анализа [24, 50, 54, 55]. Он достаточно распространен в практических приложениях и, в частности, для своего использования не требует наличия у исследователя каких-то специфических особых знаний или инструментальных средств.

Суть этого метода заключается в определении на классе исследуемых объектов по результатам их морфологического анализа совокупности морфологических классификационных признаков

(параметров) $П_1, П_2, \ldots, П_к$, характеризующих наиболее существенные структурные особенности представителей исследуемого класса объектов, и задании для каждого из этих параметров множества возможных значений:

$$\{П_{ij}\} = \{П_{i1}, П_{i2}, \ldots П_{im_i}\},\ i = \overline{1,k},\ j = \overline{1,m_i},$$

где $\{П_{ij}\}$ – морфологическое пространство i-ого признака $П_i$.

Далее определяется декартово или прямое произведение морфологических пространств всех признаков:

$$\pi = \{П_{1j}\} \times \{П_{2j}\} \times \ldots\ldots \times \{П_{kj}\}.$$

Множество π представляет собой совокупность компонентов, каждый из которых – это кортеж из *k* элементов, по одному из соответствующего исходного морфологического пространства: из $П_1$, из $П_2$,..., из $П_k$.. Это множество включает кортежи, которые представляют все возможные комбинации значений классификационных признаков (параметров) $П_1, П_2, \ldots, П_к$, образуя так называемый морфологическое сундук – общее морфологическое пространство для всего класса объектов.

Если речь идет о генерации сценариев, то каждый кортеж сформированного общего морфологического пространства представляет собой отдельный вариант сценария. Одной из основных проблем в данной ситуации является сокращение количества сгенерированных вариантов. Это обусловливает необходимость решения задачи извлечения множества неперспективных (например, маловероятных) сценариев, выделение наиболее «рациональных» вариантов, то есть перехода к селекции адекватных (реалистичных) вариантов сценариев. В научной литературе [24, 55] эта часть морфологического анализа имеет собственное название – синтез рациональных систем на морфологических множествах, чем подчеркивается его функциональное отличие от первой части метода сценариев – метода морфологического сундука.

В общем, процедура разработки сценариев, их сопоставление и анализ нуждается в решении ряда задач, особенностью которых является наличие значительного количества латентных свойств, показателей, переменных, не допускающих прямого наблюдения и

измерения, характеризующихся существенной информационной неопределенностью. В этой ситуации единственно возможным способом решения подобных задач является применение экспертных методов совместно с эффективной апостериорной обработкой полученных экспертных оценок [56-67].

При применении сценарного анализа к задачам, связанным с анализом угроз секретной информации, моментом возникновения критической (проблемной) ситуации следует считать именно реализацию определенной угрозы относительно этой информации. В соответствии с процедурой сценарного анализа, следует сгенерировать множество сценариев возможного развития событий, обусловленных реализацией угрозы секретной информации и оценить последствия развития событий по каждому из сценариев [19].

Если имеющееся множество сценариев позволяет рассчитать частный вред отдельно по каждому из них и указать частную вероятность реализации каждого, можно построить определенную иерархическую структуру, изображенную на рис. 3.4.

Фокусом Q этой иерархии является количественное значение суммарного ущерба, рассчитанного на определенном множестве независимых событий $\{Z_i\}$, $i=\overline{1,m}$, каждому из которых можно сопоставить частную вероятность p_i^* и частный ущерб q_i^*. Особенностью этой иерархии является возможность применения аппарата статистических рисков для расчета суммарного ущерба как среднего риска [27] или, по принятой в литературе по защите информации терминологией, информационного риска [68, 69]

$$Q=\sum_{i=1}^{m} p_i^* q_i^*.$$

Частные вероятности p_i^* и частные убытки q_i^* является параметрами независимых событий $\{Z_i\}$, $i=\overline{1,m}$, которые образуют первый уровень иерархии и определяются через вероятности и убытки событий, являющихся результатами развития соответствующих сценариев $\{Cu_j\}$, $j=\overline{1,k}$.

Абстрактность приведенной на рис. 3.4 структуры требует более детальных объяснений относительно формализма ее иерархии.

Прежде всего остановимся на образовании уровней 0, 1, 2 (над пунктирной горизонтальной линией) и взаимосвязей между ними, что является ключевым моментом для применения сценарного подхода к вычислению суммарного ущерба.

Предположим, что образование убытков является следствием независимого развития множества сценариев $\{Cu_j\}$, $j=\overline{1,k}$, которые разворачиваются после потери секретной информации. По истечении определенного временного интервала T результатом реализации этих сценариев становятся соответствующие независимые события V_j, которые, таким образом, являются индикаторами завершения определенных сценариев.

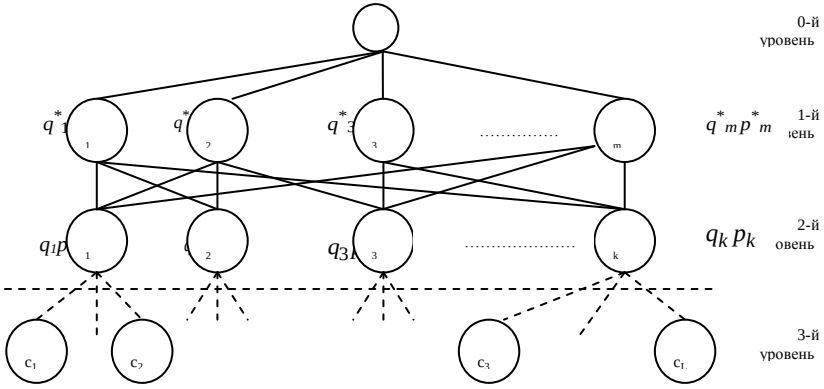


Рис. 3.4. Иерархическое представление результатов применения сценарного подхода к вычислению совокупной вреда, причиненного потерей секретной информации

Наша схема приобретает статический вид, множество событий $\{V_j\}$, для каждого из которых определена вероятность P_j (вероятность развития сценария Cu_j), образует поле событий, каждому из элементов которого может сопоставить частные убытки q_j^*. Однако непосредственное вычисление среднего риска на этом множестве невозможно из-за того, что эта совокупность событий не образует полной группы. Поэтому выполняется трансформация множества

событий $\{V_j\}$ в конечное множество $\{Z_i\}$, элементы которого соответствуют комплексу условий, обязательных для полной группы, а именно, попарной несовместности событий:

$$Z_i \bigcap Z_r = \varnothing, \quad i \neq r,$$

и второго условия:

$$\bigcup_{i=1}^{m} Z_i = \Omega,$$

где Ω – достоверное событие.

Множеству событий $\{Z_i\}$ сопоставляется множество вероятностей этих событий $\{P(Z_i)\} = \{p^*_i\}$, для которого справедливы вероятностные соотношения, характерные для элементов полной группы:

$$P(\bigcup_{i=1}^{m} Z_i) = \sum_{i=1}^{m} P(Z_i) = \sum_{i=1}^{m} p_i^* = 1,$$

$$P(Z_i \bigcap Z_r) = 0, \quad i \neq r\,.$$

Для множества событий $\{Z_i\}$ становится возможным применение аппарата средних рисков для вычисления совокупного вреда Q.

Методику образования полной группы событий рассмотрим на примере, предполагающем определенную содержательную интерпретацию, использовав для этого приведенный в Методических рекомендациях [45] пример определения степени важности информации о боевой частоте системы управления нового образца оперативно-тактической ракеты путем прогнозирования действий стороны, овладевшей этими сведениями. Пусть по результатам анализа экспертами возможных вариантов развития событий в ситуации, возникшей из-за утечки информации, наиболее вероятными являются предположения, согласно которым сторона, получившая эту информацию, использует ее для:

1) разработки средств и методов радиоподавлення системы управления ракетой;

2) планирование проведения военных операций с учетом перспектив возможной нейтрализации действий новой оперативно-тактической ракетной системы государства-противника;

3) использование полученной информации в разработке и модификации собственных оперативно-тактических ракетных систем;

4) передача информации союзникам или другим третьим сторонам.

То есть, существует четыре варианта развития событий (сценарии Cu_1, Cu_2, Cu_3, Cu_4), вероятность которых определяется частными вероятностями p_1, p_2, p_3, p_4, а завершение – событиями-индикаторами V_1, V_2, V_3, V_4. Развертывание каждого из этих сценариев связано с вполне конкретными потерями, которые понесет пострадавшая сторона, среди которых можно выделить четыре группы. Первая – финансовые затраты, связанные выполнением в максимально сжатые сроки работ по проектированию, разработке, изготовлению и компрометированного блока радиоуправления ракетой для восстановления нормального уровня боеспособности оперативно-тактических ракетных комплексов; вторая – стоимость демонтированного и замененного радиооборудования; третья – активы (финансово-экономические, технические, человеческие и т.п.), которые решено целесообразным привлечь для создания или усиления системы защиты информации; четвертая – имиджевые потери, и частности, связанные с ухудшением торговых перспектив как страны-экспортера вооружений. Полагаем, что хотя в общем случае для каждого сценария характерно наличие всех четырех видов потерь, их долевое присутствие в результирующем ущербе для того или иного сценария может быть разным, т.е. потери в отдельных сценариях не совпадают.

Выходные данные по каждому сценарию приведены в табл. 3.3. Используем эти данные для определения интегрированных потерь, обусловленных утечкой информации. События V_1, V_2, V_3, V_4, как и соответствующие сценарии, не являются несовместными, они могут происходить одновременно, а могут и не происходить совсем, то есть множество $\{V_j\}, j=\overline{1,4}$ не удовлетворяет требованиям к полной группе событий.

Поэтому возникает задача формирования полной группы $\{Z_i\}$ элементарных событий, связанных с исходным множеством $\{V_j\}$,

но, в отличие от них, удовлетворяющей требованиям, предъявляемым к полной группы.

Таблица 3.3. Исходные данные по каждому сценарию

Варианты развития сценарий, событие	Вероятность реализации	Ущерб от реализации
Cu_1, V_1	p_1	q_1
Cu_2, V_2	p_2	q_2
Cu_3, V_3	p_3	q_3
Cu_4, V_4	p_4	q_4

Каждое из событий $\{Z_i\}$ $i=\overline{1,m}$ представляет собой совмещение (комплекс) четырех элементарных событий, входящих в состав множеств $<V_1, V_2, V_3, V_4>$, $<\overline{V_1}, \overline{V_2}, \overline{V_3}, \overline{V_4}>$. Принципиальным при формировании событий $\{Z_i\}$ $i=\overline{1,m}$ является требование учета в их структуре всех возможных сочетаний элементов множества $\{V_j\}$ включая как собственно множество этих событий, так и пустое множество $\varnothing$ (если ни один из сценариев не реализовался за время T). Дальнейшее решение этой задачи практически совпадает с решением задачи, рассмотренной в п. 1.3 Модель «неопределенность – риск» в части вычисления вероятностей $P(Z_i)$. Отличия появляются при оценивании ущерба q_i^* для комплексных событий $\{Z_i\}$, $i=\overline{1,16}$. Принятие гипотезы аддитивности потерь в этой ситуации нелепо, так как ведет к их бессмысленному раздуванию, более адекватным является использование принципа «большие потери поглощают меньшие», в соответствии с которым потери для комплексного события совпадают с максимальными потерями среди четверки элементарных событий, составляющих комплекс, а $q_{16}^* = 0$. В итоге искомые потери составят

$$Q = \sum_{i=1}^{15} P(Z_i^*) q_i^*.$$

Применение изложенного метода сценариев требует отдельных методических замечаний. Прежде всего, если считать известными

значения вероятностей $\{p_j\}$ и убытков $\{q_j\}$ и не интересоваться происхождением этой информации (предположить ее абсолютный экспертный характер), то при проведении анализа по методу сценариев можно ограничиться тремя верхними уровнями схемы, изображенной на рис. 3.4. Однако при необходимости обоснования или объяснения количественных значений этих оценок возникает проблема детализации и освещение их появления, что в свою очередь вызывает возникновение дополнительных уровней предсобытий (третьего, четвертого, ..., последующих). Например, для объяснения убытков в сценариях Cu_1, Cu_2 необходимо проанализировать действия стороны, получившей информацию, и соответственно свои действия по предотвращению негативных последствий действий противной стороны, в том числе расходы на нейтрализацию и противодействие возможным военным угрозам, обусловленным утечкой информации.

Экономико-стоимостная составляющая этого анализа даст обоснование оценки ущерба, а профессионально ориентированная позволит объективно оценить остаточные вероятности угроз. То есть четвертый уровень иерархии – это взаимосвязанный перечень негативных действий противной стороны и соответствующего комплекса мер по их нейтрализации для каждого из сценариев, что позволяет проследить природу (источники) возникновения убытков и составляющие, которые формируют количественные показатели вероятностей $\{P_j\}$.

Детализация элементов четвертого уровня, например, определение конкретных механизмов и методов защиты, которые составляют комплекс защитных мер, образует нижний (пятый) уровень иерархии.

Следует заметить, что чрезмерная конкретизация в задачах прогноза, особенно с применением методов экспертного оценивания, может иногда мешать, поэтому целесообразность использования низших уровней иерархизации (от четвертого уровня и т.д.) следует определять по каждому сценарию отдельно, принимая во внимание специфику проблемной области, уровень осведомленности экспертов и тому подобное.

Кроме того, после формирования первоначального списка сценариев при переходе к анализу следует учесть возможности и результаты их взаимного влияния при условии одновременного развертывания (усиление, дополнение или взаимную нейтрализацию), т.е. проявления синергизма и эмерджентности, о которых упоминалось выше.

3.6. Применение экономико-стоимостных моделей для оценки рисков и исследования эффективности инвестиций в защиту информации

Аппроксимативные модели вероятностных параметров реализации угроз информации.

Рассмотрим ситуацию, возникающую при реализации атакующей стороной А (злоумышленник) угрозы T относительно некоторого информационного ресурса I, принадлежащего стороне В (владелец информации, организация) [18]. В общем случае вероятность P_T реализации угрозы T – это произведение [30, 17, 70]

$$P_T = P_t P_v , \tag{3.6}$$

где P_t – вероятности активации (возникновения) угрозы T, а P_v – вероятность удачного использования злоумышленником для реализации этой угрозы уязвимостей информационной системы организации В, владеющей информационным ресурсом I. Будем считать, что D – общая стоимость расходов атакующей стороны А на реализацию угрозы T, g – полученный ею при этом «выигрыш», величина которого обусловливается ценностью ресурса I для злоумышленника. Ущерб, понесенный в данной ситуации стороной В (владельцем ресурса I), определяется стоимостью критической информации с точки зрения ее владельца, оцениваемой им как q, а общая стоимость реализованного в ИС комплекса защитных мер равна c.

Приведенные выше сведения дают экономико-стоимостную характеристику ситуации «атака-защита» в ИС организации.

На базе этих сведений можно построить логико-эвристической схему экспертного оценивания вероятностных характеристик, используемых для вычисления информационных рисков.

Чистая прибыль злоумышленника в случае успешной реализации угрозы T составляет:

$$Q = g - D.$$

Если ценность ресурса I для атакующей стороны А значительна, интенсивность попыток доступа злоумышленника к ресурсу I будет очень высокой.

В частности, если $g >> D$, можно предположить, что вероятность P_t активации (возникновения) угрозы T будет практически равна 1, есть злоумышленник попытается использовать любые шансы для реализации этой угрозы.

Напротив, для малых значений g экономические мотивы возникновения угрозы T практически отсутствуют: при Q=0 (или же g=D) атака ресурса I становится нецелесообразной, в этом случае $P_t = 0$. Для g<D попытка реализации угрозы T теряет всякий экономический смысл. Исходя из этих соображений, в [51] для оценки значений вероятности активации (возникновения) угрозы T предложено соотношение:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}, \quad g \geq D. \tag{3.7}$$

Однако в выражении (3.7) никак не учитывается уровень индивидуальных характеристик злоумышленника. Поэтому более гибким является вариант оценки вероятности P_t по формуле [71]:

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g}, \tag{3.8}$$

где введен коэффициент мотивации γ, отражающий степень влияния величины ожидаемого «выигрыша» g на действия стороны А по активации угрозы T.

В зависимости от индивидуальных свойств злоумышленника коэффициент мотивации γ может быть как больше 1 (атакующей стороне А присущий азарт, авантюризм, уверенность в своем успехе), так и менее 1 (злоумышленник осторожен, не горячится, считает, что «лучше иметь синицу в руке, чем журавля в небе»). Учитывая, что значение вероятности ограничиваются диапазоном [0; 1],

на область существования значений коэффициента мотивации накладывается условие: $\gamma \geq (D / g)$.

Особенностью приведенных выше результатов является то, что они получены для гипотетического злоумышленника, который действует по принципу экономической целесообразности, это «злоумышленник-прагматик». Однако возможны и другие варианты мотивации, например, обиженный или мстительный злоумышленник («злоумышленник-мститель»), доминантой действий которого является максимизация потерь q собственника информации при условии минимальных личных расходов D. Чаще всего причиной действий этого злоумышленника являются определенные личные мотивы, обусловленные недоразумениями или конфликтными ситуациями, возникшими по месту работы, службы, прочее. Формула (3.8) в этом случае принимает вид:

$$P_t = \frac{\gamma q - D}{\gamma q} = 1 - \frac{D}{\gamma q}. \qquad (3.9)$$

Следует отметить, что приведенные выше формулы (3.8), (3.9) фактически отражают сценарии действий злоумышленника, определяемые его психотипом, причем уровень доминантной психологической характеристики злоумышленника, которая является причиной его асоциального поведения, оценивается именно коэффициентом γ. Очевидно можно выделить несколько классов психотипов злоумышленника, которые охватывают различные возможные случаи развития атаки и противоправных действий.

Другим фактором в формировании сценария действий злоумышленника может быть его социализация, в частности, его профессиональный статус. Так получаем еще один распространенный тип злоумышленника – «злоумышленника-исполнителя», который выполняет чей-то заказ или приказ, то есть атакующие действия по реализации угрозы T – это его обычная работа, которую он просто обязан выполнять. Поэтому в этом случае вероятность активации угрозы T равно $P_t = 1$.

Вторая вероятность, входящая сомножителем в произведение (3.6), P_v – это в общем случае обобщенная (интегрированная) вероятность успешного проведения комплекса атак, порожденных су-

ществованием совокупности уязвимостей ИС организации (включая уязвимости существующей СЗИ), допускающих возможную реализацию угрозы *T*. То есть значение вероятности P_v зависит от степени защищенности ИС, которая в свою очередь связана с объемом *c* инвестиций в СЗИ, что и учитывается в соотношении [72]

$$P_v = \frac{\mu q}{\mu q + sc}, \qquad (3.10)$$

где $\mu = g / q$ – коэффициент асимметрии восприятия ценности информации сторонами атаки и защиты, s – коэффициент, отражающий существующую в мировой практике зависимость между уровнем инвестиций c в СЗИ и ценностью защищаемой информации q, в частности, для информации, представляющей коммерческую тайну, возможный диапазон значений $c \approx (0{,}05 \div 0{,}20)\, q$ [69, 73]. По своей сути коэффициент s определяет уровень эффективности инвестиций c в СЗИ: чем больше значение s, тем ниже, при условии одного и того же объема c инвестиций, величина вероятности P_v. Величина s зависит от отношения организации к вопросам безопасности информации и определяется уровнем зрелости организации в сфере менеджмента безопасности информации. Получить количественную (балльную) оценку уровня зрелости можно, применив изложенную в [74] методику самостоятельного оценивания уровня зрелости системы управления рисками в организации. Найденную по этой методике балльную оценку следует использовать в качестве искомого значения s, при этом максимально возможное значение s – 85 баллов, высокий уровень зрелости организации характеризуется диапазоном 51 – 85 баллов.

Из формулы (3.10) следует, что если информационный ресурс I не интересен для злоумышленника, то в этой ситуации $g \to 0$, коэффициент $\mu \to 0$ и вероятность успешной атаки $P_v \to 0$. Если же наоборот, ресурс I не представляет особой ценности для организации-владельца, то инвестиции в СЗИ практически отсутствуют, т.е. $c = 0$, тогда $P_v = 1$. При $q >> sc$, то есть при значительном уровне ценности ресурса *I* и низких затратах на создание и функционирование СЗИ, следствием чего является объективная невоз-

можность обеспечить адекватный уровень защиты информации в ИС, вероятность $P_v \to 1$. Во всех других случаях вероятность P_v отлична от 0, а ее значение при *q=const* растет со снижением уровня инвестиций c в СЗИ.

Асимметричное восприятие ценности одного и того же информационного ресурса I атакующей и защищающейся стороной – ситуация в общем случае достаточно распространенная. Для владельца ресурса его ценность q обычно рассчитывается на основе анализа стоимостных аспектов создания этого ресурса, процедура его расчета часто носит типизированный характер, получаемые оценки достаточно устойчивы. Для атакующей стороны ценность g «добытой» информации формируется на основе изменчивой рыночной ситуации, зависящей от текущей конъюнктуры и в первую очередь от количества потенциальных покупателей, желающих заполучить ресурс I в свою собственность, в итоге $g \neq q$.

В формуле (3.10) несколько односторонне представлен ресурсный аспект противоборства сторон в ситуации «атака/защита». В общем случае вероятность успешно атаки P_v определяется соотношением потенциалов атакующей и защищающейся сторон и более полно может быть представлена эвристическим соотношением вида:

$$P_v(q,c,D) = \frac{\mu q}{\mu q + s\dfrac{c^2}{D}}, \qquad (3.11)$$

которое получено из формулы (3.10) введением мультипликатора c/D во второе слагаемое знаменателя, что позволяет сопоставить и учесть ресурсные потенциалы атакующей и защищающейся стороны: опережающий рост инвестиций в защиту ведет к уменьшению вероятности P_v, вливание инвестиций в атаку – к росту этой вероятности.

Приведенные выше формулы можно использовать как аппроксимативные модели для расчета оценочных значений вероятностных параметров P_t, P_v, что и представляло первоначальную цель их разработки [18], однако более перспективным оказалось приме-

нение полученных результатов для моделирования различных ситуаций в системе «атака/защита» при исследовании экономических аспектов проектирования, построения и функционирования СЗИ [30, 72, 75].

В последнее время большинство наиболее популярных и успешно применяемых международных и отраслевых стандартов для СМБИ: ISO 27001, ISO 27005, СТО БР ИББС, NIST SP 800-30, COSO ERM-Integrated Framework и т.д. все чаще в качестве ведущего методологического принципа выбирают риск-ориентированный подход (РОП), обеспечивающий получение определенных преимуществ в построении и эксплуатации СМБИ.

В частности, в отличие от директивного подхода к построению СЗИ, базирующегося на использовании рекомендованного перечня возможных угроз, приводящих к нарушению доступности, целостности и конфиденциальности информации, и, как правило, в полном объеме привлекаемого для формирования системы услуг безопасности при построении СЗИ, РОП позволяет из огромного количества возможных угроз и уязвимостей информационных систем выделить те, которые действительно актуальны для защиты информации в данной конкретной организации, что создает объективные предпосылки минимизации инвестиций в безопасность информации. Детальный анализ механизмов реализации выделенного ограниченного круга актуальных угроз дает возможность наилучшим образом выбрать методы и средства защиты, реально соответствующие требуемому уровню гарантий защиты и позволяет сформировать объективные инвестиционные бюджеты на создание СЗИ и СМБИ. Найденные объемы инвестиций анализируется с точки зрения эффективности СЗИ, сопоставляются с общим бюджетом организации. По результатам анализа обычно оказывается необходимым пересмотр первоначально введенных уровней гарантий защиты, внесение в них корректировок, повторное планирование и бюджетирование СЗИ, т.е. процедура анализа принимает итеративный характер. При этом в процессе итераций не должно нарушаться требование баланса рисков и инвестиций в СЗИ:

$$R_1 - R_T = P_t q - P_t P_v q = \Delta_R > c, \qquad (3.12)$$

где $R_1 = P_t q$ – исходное значение интегрального (обобщенного) риска, характеризующее возможные совокупные потери организации из-за реализации актуальных информационных угроз в случае отсутствия СЗИ,

$$R_T = P_T q = P_t P_v q, \qquad (3.13)$$

– остаточное значение интегрального риска организации, оценивающее возможные потери уже после ввода в действие СЗИ, Δ_R – предотвращенный риск, т.е. величина возможных потерь, которые удалось предотвратить благодаря созданию в организации СЗИ. Итерации прекращаются либо после достижения остаточным риском некоторого заданного минимального значения $R_{T\min}$ (или, что то же самое, уменьшению вероятность P_T реализации угрозы до заданного минимального значения $P_{T\min}$), либо после увеличения объема инвестиций в СЗИ до некоторого максимума, для которого существует очевидное ограничение $c_{\max} < q$. Учитывая, что любые объемы инвестиций в СЗИ не приведут к нулевому значению остаточного риска – это аксиома информационной безопасности, возникает вопрос: по достижению какого уровня инвестиций $c_{\max}$ следует остановить процедуру итераций? Попытка задания предельных минимальных значений вероятностей ни к чему не приведет: зависимости $R_T(c)$, $P_T(c)$ с ростом значений c спадают и на своем «выбеге» становятся очень пологими, минимальным вариациям риска R_T или вероятности P_T будет соответствовать весьма протяженный отрезок изменения аргумента c, т.е. опять придется задавать именно значение $c_{\max}$. Таким образом, актуальной проблемой становится рациональное задание уровня инвестиций $c_{\max}$.

Попытаемся оценить возможность рационального задание верхнего предела уровня инвестиций в СЗИ, исходя из условия баланса рисков и инвестиций (3.12). Подстановка выражений (3.7), (3.11) в формулу (3.13) дает возможность построить формализованную обобщенную модель интегрального риска, в которую величина c входит как параметр:

$$R(c) = (1 - \frac{D}{g}) \quad \frac{\mu q}{\mu q + s\frac{c^2}{D}} \; q. \qquad (3.14)$$

Эта же параметрическая зависимость от значений c сохранится и для величины предотвращенных потерь Δ_R, поэтому требование баланса рисков и инвестиций (3.19) можно переписать в виде $\Delta_R(c) > c$. Будем полагать, что выполнение этого условия является обязательным для эффективной СЗИ. Тогда наиболее эффективной можно считать СЗИ, для которой разность $\Delta_R(c) - c = \Delta_c(c)$, представляющая «чистую прибыль», обусловленную построением СЗИ, кажется наибольшей.

Введем понятие эффективного объема инвестиций [30, 70]:

$$c_{eff} = \arg\max_{c \in C} \Delta_c(c), \qquad (3.15)$$

где С – множество значений рациональных инвестиций c (диапазон рациональных инвестиций, диапазон «разумных» инвестиций [51, 76]), для которых $\Delta_R(c) > c$. К сожалению, получение аналитического решения c_{eff} оптимизационной задачи (3.15) после подстановка формулы обобщенной модели интегрального риска (3.14) в выражение для «чистой прибыли» $\Delta_c(c)$ в общем случае оказывается невозможным. Однако для ряде частных случаев, применяя более детальное и конкретизированное описание возможностей и свойств атакующей стороны, учитывающее мотивационно-экономические аспекты ее поведения, уровень ее компетентности и ресурсные возможности, оказывается реальным получение аналитического решения оптимизационной задачи (3.15) и ряда дополняющих это решение сведений.

Попытка определения верхнего предела необходимого уровня инвестиций в СЗИ рассматривалась в статье [77] и в ряде последовавши за ней публикаций. Авторы статьи [77], Gordon L.A., Loeb M.P., опираясь на предложенную ими модель (так называемую «модель Гордона-Лоеба»), в своих исследованиях, выполненных для достаточно общего случая, утверждают, что инвестиции в защиту не должны превышать 37% от объема максимальных потерь, возникающих в случае успешной, что реализации угроз относи-

тельно информационного ресурса *I* (фактически речь идет о 37% от ценности ресурса q), хотя обычно инвестиции существенно ниже приведенной предельной оценки. К сожалению, модель Гордона-Лоеба не поддерживает какую-либо смысловую интерпретацию в рамках прикладных исследований реальных объектов риска, конкретных механизмов возникновения и развития рисковых ситуаций, что фактически исключает возможности ее практического использования в задачах управления рисками.

Рефлексивные модели рисков

Стандарт ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [33] вводит в качестве характеристики атакующей стороны понятие «потенциала нападения», включая в него три показателя: компетентность, ресурсы и мотивации нарушителя (злоумышленника, атакующего). Исходя из этого набора показателей и учитывая, что каждый из них может иметь различную степень интенсивности, попробуем ответить на вопрос, можно ли выделить существование некоторых характерных значений этих показателей для наиболее часто встречающихся типов нарушителей. Обратимся к специальной литературе, в которой вопросы безопасности информации рассматриваются с позиций атаки и взлома информации.

Вильям Столлингс [33]: «…в действительности существует два типа хакеров. На высшем уровне находятся хорошо подготовленные специалисты, прекрасно разбирающиеся в технологии, а на низшем – «рядовые солдаты», просто использующие существующие программы взлома и имеющие весьма туманное представление о том, как эти программы работают. Эта рабочая команда объединяет два весьма грозных фактора: глубокое знание методов взлома систем защиты и тупое желание бесконечно долго «стучаться в закрытые двери», проверяя все уязвимости системы».

Данная В. Столлингсом достаточно общая характеристика атакующей стороны позволяет утверждать существование в ней двух групп, контрастных с точки зрения уровня компетентности, мето-

дов действий и используемого при этом инструментария. Попробуем уточнить и детализировать их характеристики, собрав по каждой из групп дополнительные сведения, отражающие различные аспекты поведения и подготовки атакующей стороны: выбор стратегии атаки, методы и способы реализации информационных угроз, социально-психологический контекст действий атакующей стороны, существующие (часто директивно определяемые) целевые установки этих действий. Рассматривая собранные по соответствующим группам сведения как вербальные спецификации, используем их для построения частных моделей рисков организации, подвергающейся атакующими действиями каждой из этих групп. Сформированные таким образом частные модели рисков, соответствующие введенным спецификациям, будем называть рефлексивными (от *лат. reflexus* – отображение, отражение) моделями рисков, каждой из которых присущи определенные особенности, зависящие от характеристик атакующей группы, включенных в ее спецификацию.

Подбор сведений, вводимых в спецификации, проведем, начав его с уточнения характеристик группы «рядовых солдатах» низшего уровня.

В.В. Платонов [78]: «старые угрозы реализуются атаками, базирующимися на использовании хорошо известных уязвимостей и скриптов атак (эксплойтов). Такие угрозы исходят от недостаточно компетентных хакеров (называемых ***script kiddies***) или совершенно некомпетентных (называемых ***newbies***). Эти категории нарушителей используют готовые скрипты атак и могут совершенно не понимать действительных механизмов применяемых (используемых) эксплойтов, а также их возможных побочных действий. Но это не уменьшает их опасность для организаций, так как реализация старых незащищенных угроз может нанести значительный ущерб, если организация не принимает соответствующих мер».

В соответствии с приведенной цитатой, при описании рисков, ассоциируемых с группой нарушителей низшего уровня, для моделирования вероятности P_v следует использовать модель, в которой защищенность системы от взлома определяется в первую очередь внутрисистемными факторами, характеризующими стойкость ор-

ганизации к информационным атакам, в частности, такими как уровень зрелости организации, в сфере менеджмента безопасности информации s, общий объем инвестиций в СЗИ c, стоимость критической информации с точки зрения ее владельца q. Этим требованиям в полной мере удовлетворяет формула (3.17), где характеристики атакующей стороны учитываются лишь значением коэффициента μ, в определенной степени отражающем целенаправленность и настойчивость атак.

В этом плане интерес представляет еще одно уточнение [79]: «скрипт-кидди… обычно не волнуют финансовые или политические соображения, они больше стремятся прославиться или «вызвать нарушение сервиса и породить хаос из спортивного интереса»». Другими словами, угрозы со стороны скрипт-кидди не носят целевой характер. Финансовый интерес не составляет единственную и определяющую мотивацию их действий, представления о рыночной стоимости атакуемого ресурса часто отсутствуют. Поэтому в модели (3.17) следует исключить последнюю оставшуюся возможность влияния атакующей стороны на значение вероятности P_v, положив $\mu = 1$. Кроме того, спонтанность и нецелевой характер выбора объекта атак отрицает возможность детерминированного задания значений вероятности P_t с использованием формулы (3.14), возможно более адекватным является описание P_t некоторой случайной величиной. Однако, с другой стороны, реплика Столлингса: «тупое желание бесконечно долго «стучаться в закрытые двери», проверяя все уязвимости системы» позволяет хотя бы в ряде случаев предполагать, что $P_t = 1$.

Если далее использовать термин «скрипт-кидди» как собирательный (включающий и ***newbies***), то практически все приведенные выше сведения компактно обобщаются Википедией: скрипт-кидди (англ. Script kiddie – «ребёнок, использующий скрипты» – человек, не понимающий принципов работы используемых им хакерских средств для взлома.) – в хакерской культуре название тех, кто для атаки компьютерных систем и сетей пользуется скриптами или программами чужой разработки, не понимая механизма их действия. Предполагается, что скрипт-кидди слишком неопытны, что-

бы самим написать свой собственный эксплойт или сложную программу для взлома, и что их целью часто является лишь попытка произвести впечатление на друзей или получить похвалу от сообществ компьютерных энтузиастов.

Приведенным выше обобщенным сведениям о скрипт-кидди соответствует рефлексивная модель риска вида:

$$R(c) = P_t \frac{q}{q + sc} q, \tag{3.16}$$

где вероятность удачного использования злоумышленником для реализации своих атакующих действий уязвимостей ИС организации определяется формулой

$$P_v = \frac{q}{q + sc}. \tag{3.17}$$

Из (3.17) следует, что безопасность информации в организации в первую очередь зависит от внутренних характеристик организации: суммы инвестиций c в СЗИ, уровня зрелости организации (определяется значением параметра s) и ценности q ее информационного ресурса. Рост значений параметров c и s ведет к падению значений вероятности (3.17).

По оценке А.В. Лукацкого [80], скрипт-кидди составляют до 95% от общего числа злоумышленников, атакующих информационные и компьютерные системы, т.е. это наиболее распространенный тип нарушителя, необходимость защиты от которого является первоочередной задачей, решаемой при построении СЗИ. В целом выражение для модели рефлексивного риска (3.17) намного проще общей модели риска (3.13) и допускает проведение достаточно подробных аналитических исследований. При этом особый интерес представляет сопоставление результатов исследований с известными характеристиками и показателями реальных рисков.

Рассчитав по рефлексивной модели риска (3.16) величину предотвращенных потерь $\Delta_R(c)$ (формула (3.12)) и, сопоставив ее с объемом c инвестиций в СЗИ, получим аналитическое выражение для «чистой прибыли» $\Delta_c(c)$, обусловленной построением СЗИ:

$$\Delta_c(c) = \Delta_R(c) - c = \frac{sc}{q + sc} P_t q - c. \qquad (3.18)$$

Анализ выражения (3.23) дает оценку [70] диапазона «разумных» инвестиций: $0 \le c \le q(sP_t - 1)/s$, в пределах которого $\Delta_R(c) \ge c$, а решение оптимизационной задачи (3.15), в которой выражение для $\Delta_c(c)$ задается формулой (3.18), позволяет определить эффективный объем инвестиций c_{eff}. В частности, исследуя на экстремум зависимость $\Delta_c(c)$, как функцию переменной c, приходим к уравнению:

$$\frac{d\Delta_c}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0, \qquad (3.19)$$

из которого получаем квадратное уравнение и находим его корни:

$$c^2 + 2\frac{q}{s}c + \frac{q^2}{s^2}(1 - P_t s) = 0,$$

$$c = -\frac{q}{s} \pm \sqrt{\frac{q^2}{s^2} - \frac{q^2}{s^2}(1 - P_t s)} = -\frac{q}{s} \pm \sqrt{P_t s}\,\frac{q}{s} = -\frac{q}{s}(1 \pm \sqrt{P_t s}). \qquad (3.20)$$

По своему содержанию затраты c не могут быть отрицательными, поэтому в соотношении (3.20) выражение в круглых скобках должно быть меньше нуля. С учетом этих требований, полагая, что $\sqrt{P_t s} > 1$, определяем эффективный объем инвестиций:

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1). \qquad (3.21)$$

Подставив выражение (3.21) в уравнение (3.17), получаем значение вероятности P_v в условиях эффективного объема инвестиций:

$$P_v = \frac{q}{q - q(1 - \sqrt{P_t s})} = \frac{1}{1 - 1 + \sqrt{P_t s}} = \frac{1}{\sqrt{P_t s}}. \qquad (3.22)$$

Так как $P_v \le 1$, то $1 \ge \frac{1}{\sqrt{P_t s}}$, откуда: $1 \ge P_t \ge \frac{1}{s}$, а подстановка (3.22) в выражение (3.16) позволяет найти значение риска при объеме инвестиций $c = c_{eff}$:

$$R\ (c_{eff}) = P_v P_t q = q\sqrt{\frac{P_t}{s}}.$$

Анализ формулы (3.21) дает возможность оценить максимальный объем эффективных инвестиций в СЗИ. Исследуя на экстремум зависимость (3.21) как функцию переменной *s*, получаем:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2}s^{-3/2}\sqrt{P_t}) = 0. \qquad (3.23)$$

Из равенства (3.23) определяем, экстремальное значение функции $c_{eff}(s)$:

$$\max[c_{eff}(s)] = c_{eff}(4 / P_t) = 0,25qP_t.$$

Очевидно, что наибольшей величина эффективных инвестиций в СЗИ окажется при P_t=1. Таким образом, максимальный объем эффективных инвестиций в СЗИ равен $c_{eff\,\max} = 0,25q$, т.е. составляет 25% стоимости ресурса q, являющегося объектом защиты. Однако для высокоэффективных защитных решений, что возможно при общем высоком уровне информационной культуры организации и, в частности, при высоком уровне компетентности специалистов подразделения защиты информации (например, для $s = 60$ и выше), в соответствии с формулой (3.24) даже при P_t=1 объем инвестиций в СЗИ может оказаться на уровне 11-13% от стоимости защищаемого ресурса. Условие $c \le 0,25qP_t$ можно считать формализацией принципа разумной достаточности при построении СЗИ. Кроме того, приведенный результат хорошо согласуется с эмпирическими оценками объема инвестиций в СЗИ, приведенными в ряде публикаций [69, 73], авторы которых акцентируют внимание на уровне в 15-20 % от стоимости активов ИС.

Подводя итоги рассмотрению этой рефлексивной модели риска, введем краткую вербальную спецификацию атакующей стороны.

Спецификация 1 – скрипт-кидди ***(script kiddie)***:

− скрипт-кидди характеризуются низким уровнем компетентности, не позволяющим им самостоятельно разрабатывать средства и новые оригинальные механизмы атак, более того, скрипт-кидди не понимают механизма старых атак, основывая свои атакующие действия главным образом на применении переборного принципа в реализации угроз;

− атакующая активность скрипт-кидди не носит целенаправленного характера, выбор цели и способа действий – спонтанный, объектами их атак оказываются случайные компьютеры/компьютерные системы, в руки атакующих попадает разнородная случайная информация (хотя иногда и очень ценная);

− уровень ресурсного обеспечения скрипт-кидди обычно низок и недостаточен для системной подготовки и проведения целевых атак;

− спектр интересов скрипт-кидди крайне широк и не конкретен, включая в общем случае все, что в данный момент попало в поле зрения злоумышленника и заинтересовало его, однако при этом представления как о фактической, так и о рыночной стоимости атакуемого ресурса часто отсутствуют, поэтому денежно-финансовая составляющая мотивация выражена нечетко, неустойчива, часто более весомы побуждения к действию, в основе которых лежат соображения имиджа, статусности; устойчивость и постоянство мотивации скрипт-кидди обычно проявляется лишь в самом стремлении получить несанкционированный доступ к какому-либо информационному ресурсу.

В целом для скрипт-кидди характерен низкий потенциал нападения, что позволяет для защиты от их атак применять базовый уровень обеспечения безопасности ко всем системам информационных технологий, реализуемый путем выбора стандартных защитных мер безопасности, ориентированный на применение средств и способов защиты от уже известных «старых» угроз (термин введен В.В. Платоновым, см. выше [78]).

Таким образом, если уровень квалификации атакующей стороны, ее ресурсные возможности и характер мотивации не выходят за рамки спецификации скрипт-кидди, в качестве модели риска, учитывающей основные свойства атакующей стороны, следует при-

нять модель (3.22). При этом максимальный уровень инвестиций в СЗИ организации не превышает 25% от стоимости атакуемого ресурса.

Следует отметить, что под спецификацию скрипт-кидди – спонтанно действующего некреативного злоумышленника, воспроизводящего «старые» атаки, – можно подвести различные сетевые инфекции и черви, которые в основной своей массе, исключая разработки нулевого дня, обычно успешно детектируются на базовом уровне защиты.

Расширим и детализируем характеристики второй группы атакующих, состав которой по В. Столлингсу это – хорошо подготовленные специалисты, прекрасно разбирающиеся в технологии, с глубоким знанием методов взлома систем защиты. Однако высокий уровень компетентности специалиста сам по себе еще не достаточен для подготовки и реализации «новых» опасных и предельно опасных угроз. «Некоторые методы способны обеспечить защиту от рядового пользователя, но оказываются бессильны, если атаку выполняет профессионал. А те средства защиты, которые способны остановить профессионала, необязательно являются непреодолимым препятствием для правительственного агентства крупной мировой державы» [81]. «Поэтому, если когда-нибудь разведывательное управление заинтересуется вашей компанией, приготовьтесь к тому, что против вас будут направлены огромные людские и технические ресурсы (опытные технари, новейшее аппаратное обеспечение и профессиональные шпионы)» [82]. Хотя наличие знаний и компетентности является необходимым условием формирования «новой» атаки, ее потенциал, острота, успешность в значительной степени определяются еще двумя факторами:

− во-первых, стоящая перед атакующей стороной цель или стратегическая установка (коммерческий успех, финансово-экономическая целесообразность, социально-политические или этические требования и т.п.);

− во-вторых, уровень ресурсных ограничений, возможность реализации высокозатратных атак, привлечения дополнительных кадровых, технических, оперативных ресурсов, хотя бы временно аккумулируемых для осуществления атаки.

В связи с этим расширим линейку рефлексивных моделей рисков, добавив в нее две новые модели, отражающие содержание вербальных спецификаций «злоумышленник-профессионал» и «профессионал-исполнитель», работающий на спецслужбу.

Спецификация 2 – злоумышленник-профессионал.

Атакующую сторону представляет профессионал или группа профессионалов, обладающих необходимыми знаниями, навыками и достаточным опытом, для которых хакинг – основная деятельность, носящая откровенно коммерческий характер, а целевая критериальная установка – коммерческий успех, финансово-экономическая эффективность.

Злоумышленник-профессионал обычно располагает определенными финансово-экономическими ресурсами, но для него, тем не менее, сохраняет достаточную актуальность ограничение $D \le g$.

Если стороны атаки и защиты примерно одинаково оценивают стоимость информационного ресурса I, т.е. μ=1, рефлексивная модель риска для этого случая имеет вид:

$$R(c) = (1 - \frac{D}{g}) \frac{q}{q + s\frac{c^2}{D}} q. \qquad (3.24)$$

К сожалению, подстановка найденного риска (3.24) в выражение (3.16) и последующее решения оптимизационной задачи, позволяющее получить в аналитическом виде выражение для оценки c_{eff} (как это было сделано выше для рефлексивной модели риска (3.17)), оказывается невозможным. Выражение $R_1 - R_t$ после подстановки в него риска $R_t = R(c)$ (формула (3.24)) приобретает логистический характер, а анализ неравенства $\Delta_c = R_1 - R_t - c \ge 0$ дает возможность лишь определить диапазон разумных инвестиций:

$$\frac{qP_t}{2}(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}) \le c \le \frac{qP_t}{2}(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}). \qquad (3.25)$$

Исследование соотношения (3.25) для $D = 0$ позволяет оценить граничные значения диапазона разумных инвестиций [30, 70]: $0 \le c \le q$. Наличие процедуры извлечения квадратного корня в

формуле (3.25) предполагает очевидное условие $1 \geq 4D / sqP_t^2$, трансформирующееся в ограничение вида:

$$D \leq 0,25sqP_t^2,$$

накладываемое на объем инвестиций атакующей стороны А. Кроме того, необходимость применения формулы (3.9) для оценивания вероятности активации (возникновения) угрозы T сохраняет характерное ограничение $g \geq D$. Таким образом, злоумышленник-профессионал, действующий в соответствии с принципом экономической целесообразности, ограничен возможностью проведения только низкозатратных атак. Исследование соотношения (3.25) показывает, что с увеличением значений D при $D \to 0,25sqP_t^2$ правая и левая границы диапазона (3.25) сближаются, стягиваясь в точку $c = \frac{qP_t}{2}$ для $D = 0,25sqP_t^2$, т.е. в этом предельном случае наибольшая величина оптимальных инвестиций в СЗИ составит $c_{eff\,\max} = 0,5q$. Рациональное расходование этого объема инвестиций требует проведения анализа возможных угроз безопасности информации, выделения актуальных угроз с последующей реализацией системы защитных мероприятий в форме КСЗИ в условиях оптимального распределения выделенных инвестиций.

В случае асимметричного оценивания сторонами атаки и защиты стоимости информационного ресурса I, особый интерес представляет случай, при котором $g >> q$, т.е. $\mu >> 1$. В этой ситуации атакующая сторона А может вложить в организацию и проведение атаки значительные средства, сопоставимые по величине со значением q или даже превышающие это значение. Однако при этом, если будет выполняться условие $D \leq g$, в понимании атакующей стороны выделяемый атакующий потенциал не превышает пределов экономической целесообразности. Возникает ситуация, которую можно назвать долговременной (продолжительной) целевой атакой [72]. Суть ее состоит в том, что атакующая сторона, предварительно уже выделившая изрядные ресурсы для подготовки атаки, но еще не достигшая успеха, переходит к выжидательной тактике, сопровождаемой ведением постоянного контроля за качеством

функционирования СЗИ атакуемой организации В. Рано или поздно, при возникновении локального снижения уровня ее защищенности (появление даже кратковременной уязвимости), атакующая сторона А проводит успешную атаку. Основным расходуемым ресурсом злоумышленника в этом случае является его время плюс затраты на осуществление мониторинга состояния защищенности объекта атаки.

Рефлексивная модель риска для этого случая полностью совпадает с выражением (3.20). Для выяснения особенностей рисков долговременной целевой атаки оценим предельные значения вероятностей P_t, P_v (два первых сомножителя в формуле (3.20)) в асимптотике при $g \to \infty$. Учитывая, что значение D ограничено, формально при $g \to \infty$ вероятность активации угрозы $P_t \to 1$, т.е. угроза атаки существует постоянно и ее реализация произойдет как только представится удобный момент. При наличии инсайдера в атакуемой организации именно он может сообщить о наступлении этого момента, в частности, постараться создать его. Этому моменту будет соответствовать локальный всплеск вероятности P_v, которая, согласно введенному в [30] определению, представляет собой «терминальную» вероятность, величина которой изменяется во времени в соответствии с избранной тактикой атак. Что касается оценки предельного значения вероятности P_v, то, учитывая, что с ростом g величина коэффициента асимметрии $\mu = g / q$ увеличивается, а слагаемое sc^2 / D – наоборот, с ростом D несколько уменьшается, в асимптотике при $g \to \infty$ вероятность $P_v \to 1$.

Следует отметить, что полученные выше единичные предельные значения вероятностей P_t, P_v являются лишь некоторыми асимптотическими оценочными величинами, реальность далеко не столь фатальна по отношению к защищающейся стороне. Правильный выбор стратегии защищающейся стороной, – так называемая проактивная защита, основывающаяся на упреждающих защитных действиях, опирающихся на изучение поведения, тактики и стратегии атакующей стороны, т.е. использующая подходы и принципы рефлексивного управления [72, 83] – позволяет отсрочить наступ-

ление момента успешной реализации угрозы теоретически на неограниченно долгий период времени. При этом рефлексивность действий защиты состоит, прежде всего, в осознании ею возможности асимметричного представления атакующей стороной ценности ресурса I, в частности, значительного превышения этой ценности относительно собственной оценки q. В противном случае, если защищающаяся сторона, создавая свою СЗИ, исходит из принципа разумной достаточности, основываясь исключительно на собственных («внутренних») представлениях о ценности q защищаемого ресурса I, успешная реализация угрозы атакующей стороной оказывается практически гарантированной.

Спецификация 3 – профессионал-исполнитель, работающий на спецслужбу.

Как показано в [30, 70, 72], при определенных обстоятельствах принцип экономической целесообразности может не выполняться. Именно этим ситуациям соответствует вводимая спецификация 3, описываемая ниже.

Атакующая сторона А для достижения своих целей прибегает к услугам наемного исполнителя, обязанного при любых обстоятельствах выполнять свое работу. В частности, если его задание – реализации какой-либо угрозы относительно ресурса I, то профессионал-исполнитель сразу приступает непосредственно к поиску и эксплуатации уязвимости ИС атакуемой организации, т.е. в данной ситуации $P_t = 1$. Это отличает рассматриваемую спецификацию от предыдущей, в которой атакующая сторона в своих действиях руководствовалась исключительно принципом экономической целесообразности (разумной достаточности). Особенность же Спецификации 3 состоит именно в том, что, в связи с чрезвычайной важностью поставленной перед профессионалом-исполнителем задачи, ресурсные ограничения для решения этой задачи снимаются и, кроме того, он может рассчитывать на привлечение для поддержки своих действий различных дополнительных ресурсов: финансовых, технических, информационно-аналитических, оперативных и т.п. На практике это означает возможность реализации в рамках Спецификации 3 очень высокозатратных атак ($D \to \infty$).

Типичным примером подобной ситуации является выполнение особо важного задания сотрудником спецслужбы, являющимся профессионалом, подготовленным к осуществлению атакующих действий в киберпространстве [72, 83].

Рефлексивная модель риска для этого случая проста:

$$R(c) = P_v q = \frac{q}{q + s\dfrac{c^2}{D}}\, q.$$

Из нее очевидно, что со снятием ресурсных ограничений $(D \to \infty)$ вероятность $P_v \to 1$, т.е. в этой ситуации, если защищающаяся сторона, создавая свою СЗИ, исходит из принципа разумной достаточности, основываясь исключительно на собственных («внутренних») представлениях о ценности q защищаемого ресурса *I*, успешная реализация угрозы атакующей стороной оказывается практически гарантированной и в итоге $R(c) \to q$. Это достигается за счет осуществления злоумышленником новых оригинальных атак, защиту от которых в рамках представленной в действующих руководствах по риск-менеджменту стандартной методологии, базирующейся на исследовании и анализе имевших место ранее инцидентов в сфере безопасности, осуществить практически невозможно. Таким образом, КСЗИ, построенная только в соответствии с требованиями действующих нормативных документов системы НД ТЗИ, не обеспечивает достаточных гарантий защиты от атак, реализуемых сегодня в киберпространстве, в частности, направленных целевых атак APT (Advanced Persistent Threat), динамических техник обхода AETs (Advanced Evasion Techniques), против которых применяемые комплексы традиционных защитных мероприятий малоэффективны. Перспективной в этом случае может оказаться разработка проактивных систем защиты, использующих подходы и принципы рефлексивного управления [72, 83].

Спецификация 4 – хактивист.

Атакующая сторона – идейный хакер («кибер-активист»), стремящийся перенести в киберпространство продвижения политических либо социальный идей (нередко достаточно сомнительного характера), организующий акции гражданского «электронного»

неповиновения в киберпространстве, старающийся привлечь внимание власти и общественности (иногда в довольно жесткой форме) к тем или иным вопросам и проблемам современного общества путем синтеза социальной активности и хакерства. Наиболее характерными для хактивистов акциями являются виртуальные «сидячие забастовки» и блокады, бомбардировка электронной почты, WEB-хакинг и компьютерные взломы, компьютерные вирусы и черви [80]. В действиях хактивиста практически отсутствует коммерческая составляющая, его атакующий потенциал, в частности, ресурсное обеспечение, обычно ограничены, поэтому Спецификация 4 для хактивиста, в зависимости от доступных для него ресурсов, может быть близка к Спецификации 2 или 3. Это позволяет предполагать, особенно при установлении принадлежности хактивистов к тому или иному протестному сообществу и учитывая групповой характер акции, ее тип, продолжительность, массовость, интенсивность и возможные последствия, что применение традиционных защитных мероприятий в подобных ситуациях может не быть достаточно эффективным.

Подводя итог выполненного исследования рефлексивных моделей риска, отражающих для ряда типовых ситуаций «атака-защита» характерные особенности поведения и действий атакующей стороны, приходим к следующим выводам.

Описании атакующей стороны в рамках Спецификаций 1, 2 (скрипт-кидди, злоумышленник-профессионал), позволяет осуществить анализ рисков высокого уровня, спрогнозировать оценки граничного объема инвестиций в СЗИ организации, провести приоритизацию рисков и выделение группы актуальных информационных угроз, обеспечив тем самым эффективное распределение средств, инвестируемых в СЗИ и достаточно высокий уровень защиты информации в организации.

Анализ применения риск-ориентированного подхода (РОП) к построению СЗИ организации с использованием модели рисков, определяемой в рамках Спецификации 2 для долговременных целевых атаки, приводит к выводу о необходимости применения защищающейся стороной принципов рефлексивного управления, учитывающих возможности асимметричного представления ата-

кующей стороной ценности ресурса I, в частности, значительного превышения этой ценности по сравнению с оценкой q, данной владельцем ресурса.

Учитывая, что базовая методология РОП, представленная в стандартах риск-менеджмента безопасности информации, основывается на исследовании и анализе имевших место ранее инцидентов в сфере безопасности, успешное применение РОП для построения эффективной СЗИ, позволяющей отражать новые, непрогнозируемые по имеющейся предыстории атаки, не представляется возможным. В связи с этим применения РОП для построения СЗИ от атак злоумышленников, попадающих под Спецификацию 3, является бесполезным.

Выводы о возможности реализации успешных защитных мероприятий относительно атак стороны, попадающей под Спецификацию 4 – хактивист, определяются в первую очередь возможностями ресурсной поддержки этих атак. При наличии такой поддержки хактивистом могут реализовываться высокозатратные атаки.

СПИСОК ЛИТЕРАТУРЫ К ГЛАВЕ 3

1. О.Є. Архипов, В.П. Ворожко, «Системний підхід до оцінювання ефективності захисту державної таємниці», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 10, К., С. 18-22, 2005.
2. В.В. Мельников, *Защита информации в компьютерных системах*, М.: Финансы и статистика, Электроинформ, 1997. с. 368.
3. А.Н. Морозевич, Н.Н. Говядинова, Б.А. Железко и др., *Основы экономической информатики: Учеб. Пособие*, под общ. ред., Мн.: ООО «Мисанта», 1998. с. 438.
4. В.П. Романов, *Интеллектуальные информационные системы в экономике*, М.: Издательство «Экзамен», 2003, с. 496.
5. Н.И. Кондаков, *Логический словарь – справочник*, М.: Наука, 1976, с. 720.
6. В.М. Богуш, О.К. Юдин, *Інформаційна безпека держави*, К.: «МК-Прес», 2005, с. 432.
7. В.В. Домарев, *Безопасность информационных технологий. Методология создания систем защиты*, К.: ООО «ТИД»ДС», 2001, с. 688.
8. В.Т. Циба, *Математичні основи соціологічних досліджень: кваліметрічний підхід*, К.: МАУП, 2002, с. 248.
9. С.Д. Хайтун, *Количественный анализ социальных явлений: проблемы и перспективы*, М.: КомКнига, 2005, с. 280.
10. Современное состояние теории исследования операции /Под ред. Н.Н. Моисеева., М.: Наука, 1979, с. 464.
11. А.А. Харкевич, «О ценности информации», *Проблемы кибернетики*, №4, С.14–21, 1960.
12. Р.Л. Стратанович, «О ценности информации», Изв. АН СССР. *Техническая кибернетика*, №5, С.3–12, 1965.
13. М.М. Бонгард, *Проблемы узнавания*, М.: Наука, 1967, с.320.
14. О.Є. Архипов, «Визначення цінності конфіденційної інформації», «Інтернет-освіта-наука-2010», сьома міжнародна конференція ІОН-2010, 28 вересня-3 жовтня, 2010: *Збірник матеріалів конференції*, Вінниця: ВНТУ, С.377–379, 2010.
15. О.Є. Архипов, «Теоретико-методичні засади оцінювання шкоди, обумовленої розголошенням секретної інформації», *Правове,*

нормативне та метрологічне забезпечення системи захисту інформації в Україні, Вип. №2(17), С.16-23, 2008, [Електронний ресурс], Режим доступу: http://pnzzi.kpi.ua/17/17_p16.pdf

16. О.Є. Архипов, О.Є. Муратов, *Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою, монографія*, К: Наук.-вид. відділ НА СБ України, 2011, с. 195.

17. А.Е. Архипов, «Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков», *Захист інформації*, №2 (51), С.69-76, 2011.

18. А.Є. Архипов, С.А. Архипова, «Применения мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита»», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, 1(16) вип., 2008.

19. О.Є. Архипов, І.П. Касперський, «Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, К, Вип.2 (15), С.13–19. 2007.

20. А.Н. Ефимов, *Информация: ценность, старение, рассеяние*, М.: Знание, 1978, с. 64.

21. О.Є. Архипов, «Про деякі аспекти визначення цінності конфіденційної інформації», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, Київ, випуск 2(21), С. 19-25, 2010.

22. «Государственная тайна в Российской федерации», Под ред. М.А. Вуса, СПбГУ, 1999, с. 330.

23. «Звід відомостей, що становлять державну таємницю України», К.: *Друкарня Служби безпеки України*, 2005, с. 70.

24. А.В. Катренко, *Системний аналіз об'єктів та процесів комп'ютеризації*, Львів: «Новий світ», 2000, с. 424.

25. Ю.П. Сурмин, *Теория систем и системный анализ*, К.: МАУП, 2003, с. 368.

26. Ф.Г. Коломоец, *Основы системного анализа и теории принятия решений*, Минск: «Тесей», 2006, с. 320.

27. В.С. Пугачев, *Теория вероятности и математическая статистика*, М.: Наука, Главная редакция физико-математической литературы, 1979, с. 496.

28. Г.А. Минаев, *Безопасность организации*, К.: КНТ, 2009, с. 440.

29. Г.П. Цыганенко, *Этимологический словарь русского языка*, К.: Рад.шк; 1989, с. 511.

30. О.Є. Архипов, *Вступ до теорії ризиків: інформаційні ризики: монограф*, К.: Нац. Академія СБУ, 2015, с. 248.

31. О.Є. Архипов, «Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій», *Захист інформації*, №1 (50), С.42-47, 2011.

32. А.Е. Архипов, «Технология построения комбинированных измерительных шкал для оценивания значимости информации», *Адаптивные системы автоматического управления*, № 13(33), С.153–158, 2008.

33. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», *ГОСТ Р ИСО/МЭК 15408-1-2008*.

34. О.Є. Архипов, С.А. Архіпова, *Моделювання і прогнозування в соціальній сфері: Навч.-метод. посіб.*, К.: ІВЦ Видавництво «Політехніка», 2001, с. 60.

35. О.Є. Архипов, М.А. Петренко, «Застосування онтологічної ієрархії у задачах визначення цінності інформації», *Захист інформації*, Вип. №1(54), С.45-52, 2012.

36. Т.Л. Саати, *Принятие решений. Метод анализа иерархий*, пер. с англ. Р. Г. Вачнадзе, М.: Радио и связь, 1993, с. 320.

37. S.C. Brandt, J. Morbach, M. Miatidis, M. Theissen, M. Jarke, and W. Marquardt, «An Ontology-Based Approach to Knowledge Management in Design Processes», *Computers and Chemical Engineering*, 32,1-2, pp. 320–342, 2008.

38. Н.М. Боргест, *Онтология проектирования: теоретические основы. Часть 1. Понятия и принципы/Учебное пособие*. Самара: Изд-во Самар. Гос. аэрокосм. ун-та, 2010, с. 88.

39. Н. Петренко, Krassimir Markov, Vitalii Velychko, Oleksy Voloshin, «Компьютерные онтологии и онтолого-управляемая архитектура информационных систем», *Information Models of Knowledge*, Kiev, Ukraine – Sofia, Bulgaria, С.86-92, 2010.

40. Ю.В. Рогушина, І.Ю. Гришанова, «Використання методу індуктивного виведення для вдосконалення онтології предметної області пошуку», *Системні дослідження та інформаційні технології*, №1, С.62-70, 2007.

41. Г.Л. Смилянский, Л.З. Амлинский, В.Я. Баранов и др.; Под ред. Г.Л. Смилянского, *Справочник проектировщика АСУ ТП*, М.: Машиностроение, 1983, с. 527.

42. «Информационные технологии управления», Под ред. Ю. М. Черкасова, М. :ИНФРА-М, 2001. с. 216.

43. П. Суппес, Дж. Зиннес, *Основы теории измерений, Психологическое измерение*, М.: Мир, 1976, с. 220.

44. А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*, К.: МК-Пресс, 2006, с. 320.

45. «Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності», *Державний комітет України з питань державних секретів та технічного захисту інформації*; Збірка №8, Наказ № 23 від 9 лютого 1998, К., С.4-14, 1998.

46. О.Є. Архипов, І.П. Касперський, «Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні», *Правова інформатика*, №3 (11), С. 61-66, 2006.

47. Б.Г. Литвак, *Разработка управленческого решения*, М.: Дело, 2000, с. 392.

48. Б.Є. Грабовецький, *Економічне прогнозування і планування*, К.: Центр навчальної літератури, 2003, с. 188.

49. .В. Литвиненко, *Спеціальні інформаційні операції та пропагандистські кампанії*, К.: ВКФ «Сатсанга», 2000, с. 222.

50. М.З. Згуровський, «Сценарний аналіз як системна методологія передбачення», *Системні дослідження та інформаційні технології*, №1, С. 5-36, 2002.

51. А.Б. Качинський, *Безпека, загрози і ризик: наукові концепції та математичні методи*, К., 2003, с. 472.

52. Э. Янг, *Прогнозирование научно-технического прогресса*, М.: Прогресс, 1974, с. 219.

53. Л. Жерардэн, *Исследование альтернативных картин будущего: Метод составления сценариев. Руководство по научно-техническому прогнозированию*, М.: Прогресс, 1977, с. 132.

54. Ю.М. Кузнєцов, Р.А. Скляров, Прогнозування розвитку технічних систем, К.: ТОВ «ЗМОК»– ПП «ГНОЗИС», 2004, с. 323.

55. С. Малин, В.И. Мухин, *Исследование систем управления*, М.: Издательский дом ГУВШЭ, 2004, с. 400.

56. С. Гладыш, «Организационные и методические аспекты экспертной оценки информационной безопасности информационно-телекоммуникационных систем», *Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні*, № 1(12), С.178–188, 2006.

57. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Технологии экспертного оценивания в задачах защиты информации», *Інформаційні технології та комп'ютерна інженерія*, № 2, С.89–94, 2005.

58. А.Е. Архипов, С.А. Архипова, С.А. Носок, И.В. Пишко, «Применение методов кластеризации в задаче обработки данных экспертного опроса*», Радіоелектроніка, інформатика, управління*, № 2(10), С.104–108, 2003.

59. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Применение кластерного анализа для структурирования данных экспертного опроса», *Адаптивные системы автоматического управления*, №6(26), С.55–61, 2003.

60. О.Є. Архипов, С.А. Архипова, «Модели оценивания компетентности экспертов по данным многообъектной экспертизы», *«Інтернет-освіта-наука-2010»*, сьома міжнародна конференція ІОН-2010, 28 вересня-3 жовтня 2010: Зб. мат. конф., Вінниця: ВНТУ, С.191–194, 2010.

61. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Модели компетентности експерта», *Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій* (ISMIT-2006), м. Євпаторія, 15-19 травня 2006, том 1, С.22-25, 2006.

62. А.Е. Архипов, С.А. Архипова, С.А. Носок, «О построении модели компетентности эксперта», *Системні технології. Системи управління, контролю та технічної діагностики*: Зб. наук. праць., Вип.8, Дніпропетровськ: «Системні технології», С.22-25, 2006.

63. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Модели компетентности эксперта», *Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій* (ISMIT'2006), м. Євпаторія, 15-19 травня 2006р., том 1, С. 22-25, 2006.

64. Н.Н. Китаев, *Групповые экспертные оценки*, М.: «Знание», 1975, с. 64.

65. С.А. Дубровский, *Использование экспертных оценок в задачах предварительной алгоритмизации*, М.: ЦИНИ «Электроника», 1984, с. 36.

66. Б.Г. Литвак, *Экспертная информация: Методы получения и анализа*, М.: Радио и связь, 1982, с. 184.

67. Г.М. Гнатієнко, В.Є. Снитюк, *Експертні технології прийняття рішень: Монографія*, К.: ТОВ «Маклаут», 2008, с. 444.

68. С.В. Симонов, «Методология анализа рисков в информационных системах», *Защита информации*, №2, С. 48-53. 2001.

69. С. Петренко, С. Симонов, *Управление информационными рисками. Экономически оправданная безопасность*, М.: Компания Ай-Ти, ДМК Пресс, 2004, с. 384.

70. А.Е. Архипов, «Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации», *Захист інформації*, Том 17, №3, С.211-218, 2015.

71. А.Е. Архипов, А.В. Скиба, «Практические аспекты оценивания рисков реализации угроз в информационных системах», *Захист інформації*, Том16, №4, 2014.

72. А.Е. Архипов, «Применение рефлексивных моделей рисков для защиты информации в киберпространстве», *Захист інформації,* Том 19, №3, С. 204-213, 2017.

73. Г.А. Андрощук, П.П. Крайнев, *Экономическая безопасность предприятия: защита коммерческой тайны*, К.: Изд. Дом «Ин Юре», 2000, с. 400.

74. «Руководство по управлению рисками безопасности» [Электронный ресурс], *Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам; Центр Microsoft security center of excellence*, TechNet, Редмонд, США: Корпорация Майкрософт, 2006, [Online]. Режим доступа:

http://technet.microsoft.com/ru-ru/library/cc163143.aspx. – [просмотрено 29 декабря 2011].

75. А.Е. Архипов, «Экспертно-аналитический подход к оцениванию информационных рисков», *Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту*: Матеріали міжнародної наукової конференції (ISDMSI'2009), Том 1, Херсон: ХНТУ, С. 246-249, 2009.

76. В. Гранатуров, *Экономический риск: сущность, методы измерения, пути снижения*, М. : изд-во «Дело и Сервис», 1999, с. 112.

77. Lawrence Gordon and Martin P. Loeb «The Economics of Information Security Investment», *ACM Transaction on Information and System Security*, Vol.5, No4, November, P. 438-457, 2002.

78. В.В. Платонов, *Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей*, М.: «Академия», 2006, с. 240.

79. Dorothy E. Denning. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy // *Global Problem Solving Information Technology and Tools*, December 10, 1999, https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

80. А.В. Лукацкий, *Обнаружение атак*, СПб.: БХВ, Петербург, 2003, с. 608.

81. Д.В. Скляров, *Искусство защиты и взлома информации*, СПб.: БХВ-Петербург, 2004, с. 288.

82. Д. Макнамара, *Секреты компьютерного шпионажа: Тактика и контрмеры*. М.: БИНОМ. Лаборатория знаний, 2004, с. 536.

83. А.Е. Архипов, «Экономические аспекты информационной безопасности», *Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту* (ISDMCI'2016, Залізний порт, 2016 р.): Матеріали міжнародної наукової конференції, Херсон: Видавництво ПП Вишемирський В.С., С.23-25, 2016.

Глава 4. ОБРАБОТКА РЕЗУЛЬТАТОВ ЭКСПЕРТНОГО ОЦЕНИВАНИЯ

4.1. Экспертное оценивание, общие сведения

Экспертное оценивание – издавна одна из самых распространенных информационных технологий, которая и в наше время привлекает широкий круг специалистов – как практиков, так и теоретиков. Объясняется это рядом особенностей, присущих методу экспертных оценок.

Во-первых, данный метод – наиболее доступный, универсальный, а иногда просто единственно возможный для получения и анализа информации, используемой для решения широкого спектра задач управления, прогнозирования, планирования в науке, технике, различных практических приложениях.

Во-вторых, сфера использования экспертного оценивания постоянно расширяется, в частности, это – определение параметров и структуры сложных систем, особенно тех, которые не имеют достаточной предыстории функционирования и характеризуются высоким уровнем структурно-параметрической неопределенности: сложных социально-экономических систем, систем проектного менеджмента, СЗИ и т.д.

Общей, достаточно привлекательной стороной экспертных методов является оперативность и простота получения нужных сведений.

При использовании метода экспертных оценок основным источником информации является эксперт – его суждения, качественные и количественные оценки. То есть экспертные методы основаны исключительно на оценках экспертов, полученных относительно проблемы, которую они исчерпывающе знают. При этом механизм выработки этих оценок остается неопределенным. Как правило, он неизвестен даже самому эксперту, имеет исключительно индивидуальный, личный характер и не может быть повторен или воспроизведен кем-то другим. Это обусловливает особые требования к выбору состава экспертов, в частности уровня их компетентности, ведь недостаточный уровень компетентности эксперта может привести к появлению грубых (аномальных) ошибок в данных экспертизы или просто вызвать высокий уровень неоднород-

ности этих данных. В обоих случаях возможны существенные потери информации, которые приведут к неправильно принятым по результатам экспертизы решениям, ложному задания параметров, оценок и т.п., то есть негативные последствия некачественно выполненной экспертизы могут быть ощутимы и на всех последующих этапах применения результатов, полученных по экспертным данным.

Поэтому эффективная, качественная обработка экспертных данных в значительной степени определяет корректность и правильность выполнения всей экспертизы в целом. В этой ситуации особую важность и актуальность приобретает проблема анализа и обработки экспертной информации, так как выполнение именно этих процедур позволяет обеспечить качество решений, принимаемых на базе экспертной информации.

Отсутствие общепризнанных формально-теоретических и методологических положений, объясняющих механизм формирования экспертных данных (в том числе и ошибок в этих данных), обусловливает тот факт, что общие рекомендации по обработке экспертных данных, тем более реализованные в форме программного продукта, на сегодня отсутствуют. Обработчик, использующий экспертные данные, чаще всего сам решает, как с ними работать. Применяемые математические методы обработки экспертных данных, как правило, очень просты, ибо использование более сложных методик обработки требует привлечения дополнительной информации, обычно отсутствующей.

Все сказанное выше обусловливает актуальность исследований, связанных с изучением и разработкой методов или методик обработки экспертных данных. Особенно актуальна проблема обработки данных экспертизы в новых сферах человеческой деятельности, в которых еще недостаточно сформировался формально-теоретический базис, не структурировано разнообразие свойств и особенностей изучаемых объектов, не сформировалось достаточное количество специалистов, адекватных по качеству своей подготовки требованиям, предъявляемым уровню эксперта.

Чем «моложе» предметная область и динамичней ее развитие, тем в общем случае чаще приходится применять экспертные методы решения задач этой области и тем сложнее сформировать груп-

пу экспертов, имеющих одинаково высокий уровень компетентности. К сожалению, организаторы экспертизы часто осознают эту проблему только после ознакомления с полученными экспертным данным, когда эти данные оказываются единственным «сырьем», из которого можно получить необходимые сведения об уровне компетентности каждого эксперта.

Методы получения экспертных оценок делятся на две группы: индивидуальные (персональные) экспертизы и групповые (коллективные) процедуры получения экспертных оценок.

Среди методов получения индивидуальных экспертных оценок, в свою очередь, выделяются: метод аналитических записок, интервью, анкетирование и т. п.

Методы коллективной экспертизы – соответственно метод комиссии, метод Дельфи, паттерн и другие.

Разделение на методы получения индивидуальных и коллективных экспертных оценок проводится в зависимости от того, как определяется конечный результат экспертизы: на основе выводов одного эксперта или по результатам работы группы экспертов, причем результат групповой экспертизы в некоторых случаях может формироваться путем интеграции индивидуальных оценок экспертов.

Главной проблемой любой экспертизы является выбор способа формирования суждений экспертов. Именно этот вопрос должен иметь первоочередной приоритет в анализе, исследовании и разработке различных аспектов экспертизы, связанных с ее организацией и проведением. Частично эти проблемы уже рассматривались выше, когда речь шла о критериях отнесения информации к секретной, формировании структуры и выбор составляющих элементов соответствующего критериального показателя, способах определения его количественных оценок экспертами (МАИ, нониусный подход, технологии нечетких множеств). Несколько меньшее внимание уделяется средствам и методам уменьшения погрешностей в совокупности уже полученных индивидуальных оценок, в частности при их интеграции в конечный результат групповой экспертизы.

В работе [1] приведено описание ряда распространенных методов экспертной оценки с элементами их анализа с точки зрения

возможности обеспечения информативности и точности результатов экспертизы. По материалам этого обзорного исследования можно сделать вывод, что, несмотря на различия рассмотренных методов, им присущ ряд общих технологических особенностей (мер, приемов, процедур), направленных на повышение информативности и точности экспертных данных. Анализируя совокупность этих мер, приемов можно выделить такие основные направления повышения качества результатов экспертизы:

- определение необходимых и достаточных условий для оценки специалиста как эксперта;
- оценки характеристик эксперта;
- организация проведения экспертизы;
- выбор методов стимулирования экспертов;
- выбор методов обработки экспертной информации и другие.

Обобщение приведенных в работе [1] материалов позволяет выделить три основные группы методов уменьшения погрешности экспертных оценок:

- организационные методы – базируются на внедрении специальных организационных процедур по получению и использованию дополнительной информации, применяемой для обеспечения высокого уровня достоверности проводимых экспертиз (прежде всего, это так называемые «сложные экспертизы», в частности «дельфийская», в которых непосредственно применяются такие организационные формы проведения экспертирования, которые гарантированно обеспечивают высокую конечную точность результатов экспертизы);
- организационно-расчетные методы – суть их заключается во введении специальных организационных мероприятий по получению дополнительной информации об уровне компетентности экспертов и использовании этой информации в процессе дальнейшей специальной обработки результатов экспертизы;
- математические методы обработки данных экспертизы, основанные исключительно на добыче и последующем использовании вспомогательной информации непосредственно из результатов экспертизы, без применения специальных организационных мероприятий и процедур на этапах подготовки и проведения экспертирования.

Анализируя наиболее распространенные методы экспертного оценивания, стоит сосредоточить внимание на временном и стоимостном аспекте их применения. Сложные экспертизы (например, метод Дельфи) требуют проведения достаточно кропотливой организационной работы, которая и позволяет обеспечить и качество, и надежность выходных результатов экспертизы. Сама процедура сложной экспертизы занимает довольно много времени (например, опять-таки дельфийская процедура). В совокупности и временной фактор, и организационный обусловливают высокую стоимость экспертизы. Однако выше уже отмечалось, что к экспертным оценкам обращаются именно из-за возможности сэкономить и время, и средства. Поэтому использование сложных экспертиз противоречит самой логике побудительных мотивов, обусловливающих обращение к этим процедурам. Значительно чаще обращаются к простым экспертизам, более быстрым и оперативным, при этом необходимое качество их результатов обеспечивается проведением апостериорной математической обработки полученных оценок.

Ниже рассмотрим некоторые устоявшиеся и методически обеспеченные способы проведения экспертизы и обработки ее результатов.

4.2. Получение и обработка оценочных суждений членов экспертных комиссий при государственных экспертах по вопросам тайн

В соответствии с Законом Украины «О государственной тайне» [2], отнесение информации к ГТ – это процедура принятия государственным экспертом по вопросам тайн (ГЭТ) решения об отнесении категории сведений или отдельных сведений к ГТ с установлением степени их секретности путем обоснования и определения возможного ущерба национальной безопасности Украины в случае разглашения этих сведений, включением этой информации в ССГТ, с опубликованием этого Свода и последующих изменений, вносимых в него.

Для выполнения поставленных перед ними задач ГЭТ могут, в частности, создавать экспертные комиссии (ЭК) из специалистов и ученых, имеющих допуск к ГТ, для подготовки проектов решений об отнесении информации к ГТ, снижению степени ее секретности

и отмене указанных решений. Кроме названных задач, к компетенции этих комиссий, в соответствии с «Положением об экспертной комиссии по вопросам государственной тайны» (далее – Положение [3]), отнесено определение и изменение степени секретности (СС) информации, отнесенной к ГТ.

Положением [3] закреплены только целевые установки, полномочия и общие организационные основы работы ЭК по вопросам ГТ. Документом, которым установлен порядок отнесения сведений к ГТ и установления степени их секретности в Украине, являются Методические рекомендации [4]. Несмотря на наличие упомянутых выше документов, к сожалению, до сих пор остается не решенным ряд вопросов, напрямую влияющих на эффективность деятельности ГЭТ. Прежде всего, это отсутствие каких-либо регламентаций по способу определения экспертами количественных оценок объекта экспертизы и порядка обобщения оценочных суждений членов ЭК [5].

Сейчас в трудах отечественных и зарубежных ученых исследуются методические проблемы деятельности экспертных групп и применения экспертных оценок для решения широкого круга задач, в том числе прогнозирования социальных явлений [6-8]. Анализ этих имеющихся научных результатов позволяет сделать вывод о возможности их использования после соответствующей адаптации в заполнении пробелов методического обеспечения деятельности ЭК при ГЭТ.

Отметим, что применение метода опроса экспертов для прогнозирования возможных последствий разглашения информации, в том числе их тяжести, полностью соответствует традиционной сфере использования этого научного инструмента, так как он преимущественно используется для анализа и оценки объектов высокой сложности в условиях недостаточно сформированного инструментария описания и исследования этих объектов, при отсутствии единой логико-математической структуры, учитывающей все многообразие свойств исследуемых объекта [9].

В соответствии с Методическими рекомендациями [4] для определения принадлежности сведений к ГТ специально созданными для этой цели ЭК при ГЭТ рассчитывается уровень потенциального совокупного ущерба государству в определенных законодатель-

ством сферах путем учета ряда показателей, которые определяются членами ЭК и заносятся ими в индивидуальные опросные листы, включающих следующие вопросы:

1) сведения, подлежащие экспертизе;

2) сфера или сферы деятельности, к которой относятся сведения;

3) объект, который содержит сведения, подлежащие экспертизе, их удельный вес (в баллах);

4) прогнозные действия стороны, которая несанкционированно ознакомилась со сведениями;

5) составная часть объекта (СЧО), непосредственно подпадающая под возможные воздействие стороны, которая овладела секретными сведениями;

6) снижение эффективности использования СЧО или объекта в целом вследствие действия стороны, овладевшей секретными сведениями;

7) величина экономического ущерба (в баллах), связанного со снижением эффективности использования СЧО или объекта в целом;

8) иные тяжкие последствия от потери секретных данных, уровень причиненного в результате этого ущерба (в баллах);

9) совокупная вред (в баллах).

Согласно разделу 5.1 Методических рекомендаций [4], содержание пунктов 2-5 опросного листа определяются членами ЭК совместно. Это обусловливает возможность объективизации индивидуальных оценок экспертов по этим пунктам в ходе их обсуждения. Однако выводы по пунктам 6-9 каждый член ЭК делает независимо друг от друга. Таким образом, по характерным особенностям работы комиссии, выполняемую ею экспертизу следует считать групповой (коллективной, коллегиальной), окончательное количественное экспертное заключение которой определяется на базе обработки предварительно полученных индивидуальных экспертных оценок. Процедуру этой обработки в Методических рекомендациях [4] сведено к вычисления среднеарифметического значения соответствующих индивидуальных оценок.

К сожалению, среднеарифметическая оценка очень чувствительна к так называемым аномальным данным, то есть данным, которые по своим значениям «выпадают» из общей совокупности

экспертных оценок (от англоязычного outstanding date). В частности, если хотя бы один из экспертов, входящих в состав ЭК (по пятому разделу Методических рекомендаций [4] численность ЭК – 5-7 человек или более) даст количественную оценку, существенно отличную от других, это приведет к заметному смещению среднеарифметического, особенно ощутимому при минимальном количестве экспертов. Например, в случае формального выполнения требований Методических рекомендаций [4], по полученной совокупности {85, 90, 90, 95, 160} значений балльных оценок объект экспертизы, согласно шкале, введенной в п. 3.3 настоящих Методических рекомендаций [4], должен получить СС «ОВ» (среднеарифметическая оценка равна 104 и попадает в пределы «от 100 и более», что соответствует степени «ОВ»), тогда как первые четыре эксперты единодушно определили целесообразность степени «СС» (среднеарифметическая оценка первых четырех экспертов равен 95 баллов и попадает в пределы «от 10 до 100 баллов», что соответствует «СС») [10].

Опираясь на приведенный пример, можно констатировать, что положения Методических рекомендаций [4] по обработке индивидуальных оценок экспертов не рассчитаны на возможность наличия оценки с существенным отклонением от уровня других оценок и гарантируют приемлемые результаты только в случае, когда индивидуальные оценки экспертов образуют более или менее однородную совокупность. Очевидно, в реальности возникновения ситуации, подобной приведенному примеру, становится причиной дополнительного неформального обсуждения экспертами объекта экспертизы, то есть фактически появляется второй тур экспертизы, в котором осуществляется выявление особенностей объекта экспертизы, породивших противоречивые оценки, попытка установления взаимопонимания и, как следствие, возможное сближение индивидуальных экспертных оценок.

Несовершенство среднеарифметического как интегрального показателя, исчисляемого по совокупности индивидуальных оценок экспертов, – достаточно известный факт. В качестве альтернативы среднеарифметическому чаще всего применяется медианное среднее или специальная двухэтапная методика обработки совокупности индивидуальных оценок, согласно которой на первом этапе, на

множестве индивидуальных экспертных оценок выявляются и исключаются из дальнейшей обработки аномальные данные, что позволяет на втором этапе применить среднеарифметическое для формирования интегральной оценки групповой экспертизы.

Дальнейшим развитием этой методологии можно считать так называемое взвешенное среднее. В этом подходе система специально рассчитанных весов, в которых зафиксирован уровень доверия к индивидуальным оценкам экспертов, позволяет дифференцировать вклад каждой отдельной экспертной оценки в совокупную групповую (интегральную). При этом максимальный вклад приходится на индивидуальные оценки, полученные от более опытных и компетентных экспертов, минимальный – на оценки, полученные от экспертов с самым низким уровнем компетентности. Если определенному эксперту соответствует нулевой или близкий к нулевому вес, это фактически означает, что его данные изымаются из обработки, что и происходит в случае, когда индивидуальная экспертная оценка представляет собой аномальные данные.

Проблемным аспектом взвешенного среднего является объективизация определения весов экспертов, успешность которой в свою очередь обусловлена степенью эффективности процедуры оценки уровней компетентности экспертов. Ниже рассмотрены некоторые подходы и способы решения этих двух задач.

4.3. Способы формирования групповых экспертных оценок

Одним из ключевых вопросов обработки экспертных данных является определение уровня показателя компетентности экспертов и учета этого уровня при окончательной обработке результатов экспертизы. Особый вес показателя компетентности обусловлена тем фактом, что единодушие выводов экспертов по проблеме, которая анализируется, – это возможное свидетельство или тривиальности исследуемой проблемы, или отсутствие возможности свободного выражения каждым из экспертов своего личного мнения об объекте экспертизы. Принципиальной особенностью процедуры экспертизы является возможность получения для объекта экспертизы существенно отличных или даже несовместимых оценок, и как следствие этого – проблема корректного синтеза окончательного экспертного заключения, решение которой возможно

только с учетом объективно определенного уровня компетентности экспертов.

Конкретизируем задачу [11]. Предположим, что цель экспертизы - определение уровня важности предназначенных для экспертизы нескольких информационных продуктов (информационных блоков, единиц, объектов и т.д.), например, трех: $П_1$, $П_2$, $П_3$. Каждый из них эксперты $E_1,\ldots, E_n$ оценивают в количественной шкале *0–L* баллов. Более важному объекту экспертизы присуждается большее количество баллов. По результатам групповой экспертизы каждый из объектов экспертизы получает определенную сумму баллов:

$$Q_t = \sum_{i=1}^{n} q_{it} \qquad (4.1)$$

или соответствующий средний балл:

$$\overline{q}_t = \frac{1}{n}\sum_{i=1}^{n} q_{it} = \frac{1}{n} Q_t,$$

где q_{it} – оценка, которую дал эксперт $E_i, i = \overline{1,n}$ информационному продукту $П_t$, $t = \overline{1,3}.$ Если не принимать во внимание уровни компетенции экспертов, наиболее важным будет объект экспертизы с наибольшей суммой баллов Q, или с самым высоким средним баллом $\overline{q}$.

Учет компетентности экспертов в подобной ситуации чаще всего реализуется путем введения специальных весовых коэффициентов ω_i, значения которых зависят от уровня компетенции C_i соответствующего эксперта, причем более компетентному эксперту соответствует больший весовой коэффициент. На совокупность весовых коэффициентов накладывается так называемое требование несмещенности

$$\sum_{i=1}^{n} \omega_i = 1, \qquad (4.2)$$

смысл которой заключается в том, что в случае, когда все эксперты дали объекту одинаковую оценку q, взвешенный средний балл совпадает с этой оценкой:

$$\overline{q}_t = \sum_{i=1}^{n} \omega_i q_{it} = q \sum_{i=1}^{n} \omega_i = q. \qquad (4.3)$$

Чтобы вес ω_i зависел от C_i и одновременно выполнялось требование несмещенности (4.2), значение ω_i рассчитываются по формуле:

$$\omega_i = \frac{C_i}{\sum_{j=1}^{n} C_j}.$$

Отметим, что средневзвешенный балл $\overline{q}_t$ можно найти по формуле:

$$\overline{q}_t = \frac{\sum_{i=1}^{n} C_i q_{it}}{\sum_{i=1}^{n} C_i} = \frac{1}{\sum_{i=1}^{n} C_i} Q_t^{(k)}, \qquad (4.3^*)$$

где $Q_t^{(k)}$ – суммарный балл, полученный t-им объектом с учетом уровня компетентности $C_i, i = \overline{1,n}$.

Как определить уровень компетентности? Наиболее просто и оперативно это можно сделать методом взаимо- и самооценивания экспертов (метод взаимо- и самоанализа), в котором каждый из экспертов E_1, $E_2, \ldots, E_n$ определяет свой уровень компетентности и всех других экспертов в определенной количественной шкале. Усреднение оценок уровня компетентности, полученных каждым из экспертов, дает усредненную компетентность соответствующего эксперта:

$$\overline{Z}_i = \frac{1}{n} \sum_{j=1}^{n} z_i(E_j), i = \overline{1,n},$$

где $z_i(E_j)$ – оценка уровня компетентности *i*-го эксперта, определенная *j*-м экспертом, в случае $i = j$ имеем самооценку $z_i(E_i)$.

Недостатком этого метода является возможное субъективная окраска полученной средней компетентности, что обусловлено, например, принадлежностью экспертов к противоположным научным школам или направлениям, личная неприязнь, возрастные различия и т.п.

С этих позиций более приемлемым можно считать так называемый документационный метод оценки уровня компетентности, основанный на возможной связи компетентности эксперта с такими его личными документированными данными, как число публикаций по тематике экспертизы, количество ссылок на его публикации, сфера специализации эксперта, уровень его осведомленности о положении дел в области экспертирования, опыт практической работы в этой области в ранге исполнителя, руководителя и другие данные, объективно характеризующие личность эксперта. Считается, что приведенные выше факторы (определим их идентификаторами $f_1, f_2, \ldots$) влияют на формирование уровня компетентности C_i эксперта E_i, и это может быть отражено в известной линейной форме:

$$C = a_1 x_1 + a_2 x_2 + \ldots + a_k x_k, \qquad (4.4)$$

где коэффициенты влияния a_k фиксируют уровень влияния факторов $f_1 = x_1, \quad f_2 = x_2, \ldots,$ или зависимых от этих факторов переменных $x_l = \phi_l(f_1, f_2, \ldots), \ \ldots, x_k = \phi_k(f_1, f_2, \ldots)$ на уровень C_i компетентности i - ого эксперта.

К сожалению, в этой ситуации опять же весьма существенен субъективный фактор, на этот раз проявляющийся при выборе значений коэффициентов влияния $a_j, j = \overline{1,k},$ причем степень субъективизма в данном случае еще выше, чем в первом случае.

Возможное положительное решение проблемы определения уровней компетентности экспертов заключается в совмещении обоих приведенных выше методов путем построения модели компетентности экспертов, которая связывает оценки усредненной

компетентности $\bar{Z}_i$ с объективными документальными данными об экспертах. Считаем, что

$$\bar{Z} = C + \xi,$$

где ξ – случайная субъективная погрешность в оценке уровня компетентности эксперта.

После подстановки

$$C = \bar{Z} - \xi$$

в уравнение последнее приобретает форму линейной регрессии:

$$\bar{Z} = a_1 x_1 + a_2 x_2 + ... + a_k x_k + \xi,$$

единственным отличием которой от ранее рассмотренных является гетероскедастичность зависимой переменной $\bar{Z}$, то есть непостоянство дисперсии ее оценок $D\{\bar{Z}\}$. В этом легко убедиться, подсчитав дисперсии оценок Z_i, $i = \overline{1,n}$, полученных каждым из экспертов:

$$D\{\bar{Z}_i\} = \sigma_z^{\,2} \approx \frac{1}{n-1}\sum_{j=1}^{n}\left[Z(E_j) - \bar{Z}_i\right]^2,$$

которые могут иметь весьма существенные разногласия.

Соответствующие дисперсии средних будут в n раз меньше, однако относительный уровень расхождения их значений останется без изменений. Вектор оценок регрессионных коэффициентов в этом случае оценивается по формуле:

$$\tilde{A} = \left(X^T W X\right)^{-1} X^T W Z,$$

где W – весовая матрица,

$$W = D^{-1},\ D = \begin{vmatrix} D\{\bar{Z}_1\} & 0 & ... & 0 \\ 0 & D\{\bar{Z}_2\} & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & D\{\bar{Z}_n\} \end{vmatrix}.$$

Несколько иным способом расчета вектора $\tilde{A}$ является переход к так называемой взвешенной регрессии:

$$V = a_1 u_1 + a_2 u_2 + ... + a_k u_k + v,$$

коэффициенты которой вычисляются обычным методом наименьших квадратов из переопределены системы взвешенных уравнений:

$$\begin{cases} \dfrac{\bar{Z}_1}{\sqrt{D\{\bar{Z}_1\}}} = a_1 \dfrac{x_{11}}{\sqrt{D\{\bar{Z}_1\}}} + ... + a_k \dfrac{x_{1k}}{\sqrt{D\{\bar{Z}_1\}}} + \dfrac{\xi_1}{\sqrt{D\{\bar{Z}_1\}}} \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ \dfrac{\bar{Z}}{\sqrt{D\{\bar{Z}_n\}}} = a_1 \dfrac{x_{n1}}{\sqrt{D\{\bar{Z}_n\}}} + ... + a_k \dfrac{x_{nk}}{\sqrt{D\{\bar{Z}_n\}}} + \dfrac{\xi_n}{\sqrt{D\{\bar{Z}_{1n}\}}} \end{cases} . \quad (4.5)$$

Принимая во внимание, что $\sqrt{D\{\bar{z}_i\}} = \sqrt{\frac{1}{n} D\{z_i\}} = \frac{1}{\sqrt{n}} \sigma_{Z_i}$, и множитель $\frac{1}{n}$ выносится из-под радикала в знаменателях системы (4.5) и сокращается, процедуру взвешивания исходных данных в векторно-матричной форме можно представить соотношениями:

$$V = T^{-1}\bar{Z} = \begin{vmatrix} \bar{Z}_1 / \sigma_{Z_1} \\ ... \\ \bar{Z}_n / \sigma_{Z_n} \end{vmatrix},$$

$$U = T^{-1}X = \begin{vmatrix} x_{11} / \sigma_{Z_1} & ... & x_{1k} / \sigma_{Z_1} \\ ... & ... & ... \\ x_{n1} / \sigma_{Zn} & ... & x_{nk} / \sigma_{Z_n} \end{vmatrix},$$

где $TT^T = nD$,

$$T = T^T = \begin{vmatrix} \sigma_{Z_1} & 0... & 0 \\ 0 & \sigma_{Z_2} ... & 0 \\ 0 & 0... & \sigma_{Z_n} \end{vmatrix},$$

$$T^{-1}=\begin{vmatrix} 1/\sigma_{Z_1} & 0 & \dots & 0 \\ 0 & 1/\sigma_{Z_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1/\sigma_{Z_n} \end{vmatrix}.$$

После взвешивания элементы вектора $V^T=[v_1,v_2,...,v_n]$ будут иметь одинаковую дисперсию, то есть это будет гомоскедастическая переменная и вектор оценок регрессионных коэффициентов определится по традиционной для метода наименьших квадратов формуле:

$$\tilde{A}=\left(U^TU\right)^{-1}U^TV\,.$$

Когда будет найдена модель (4.4) зависимости уровня компетентности экспертов от их личных документальных данных, можно будет, подставив в нее соответствующие наборы значений регрессоров $X_i=[x_{i1},x_{i2},...x_{ik}]$, найти оценки компетентности $\tilde{C}_i=X_i\tilde{A}$ экспертов E_i, $i=\overline{1,n}$ и далее, используя формулы (4.1), (4.3), (4.3*), вычислить результаты экспертизы, т.е. q_t или $Q_t^{(k)}$, $t=\overline{1,3,}$ и определить важность каждого из объектов экспертизы.

4.4. Оценка качества работы экспертов по данным многообъектной экспертизы

Среди множества экспертных технологий, привлекаемых для решения различных задач, можно выделить достаточно распространенный вид коллективной экспертизы, которая называется многообъектной экспертизой (МОЭ) [12, 13]. В МОЭ участвует группа из *N* экспертов, каждый из которых осуществляет индивидуальную экспертизу *M* объектов, составляющих экспертируемую совокупность. Полученные в ходе индивидуальных экспертиз подмножества (столбцы) из *M* экспертных оценок сводятся в общую матрицу данных, подлежащих последующей совместной обработке:

$$Z = [z_{ij}] = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1N} \\ z_{21} & z_{22} & \dots & z_{2N} \\ \dots & \dots & \dots & \dots \\ z_{M1} & z_{M2} & \dots & z_{MN} \end{bmatrix} = [Z_1, Z_2, ..., Z_N].$$

Особенностью МОЭ являются достаточно большие объемы M объектов, подлежащих экспертизе, в качестве которых могут выступать образцы определенных типов продукции, изделий, информационные продукты (в частности, программное обеспечение), художественные или литературные произведения, ответы на списки вопросов (опросники) в социологических или психологических исследованиях, присланные на конкурс проекты и т.п. В частности, работа постоянно действующих групп (комиссий) экспертов, действующих в определенной профессиональной сфере, реализующих экспертизу более-менее устоявшегося класса (или классов) информационных продуктов, является типичным образцом МОЭ. Полученные в этом случае относительно большие объемы индивидуальных экспертных оценок среди прочего содержат определенную информацию о личных качествах экспертов, в частности, об уровнях их компетентности, знание которых весьма актуально для организации эффективной обработки результатов экспертизы. Поэтому перспектива оценки компетентности эксперта, непосредственно по результатам проведенной им экспертизы, учитывающая, в том числе и состояния эксперта на момент проведения экспертизы, является весьма привлекательной.

Результаты индивидуальной экспертизы, проведенной j-м экспертом, представляют собой случайную последовательность $Z_j = [z_{1j}, z_{2j}, ..., z_{Mj}]^T$, каждый элемент которой содержит информативную составляющую x_{i0}, общую для всех экспертных оценок z_{ij} и случайную погрешность e_{ij}, характеристики которой индивидуальны у каждого конкретного эксперта:

$$z_{ij} = x_{i0} + e_{ij},\ i = \overline{1, M},\ j = \overline{1, N}.$$

Поставив в соответствие элементам последовательности Z_j целочисленные моменты времени $t_i = 1, 2, ..., M$, получим некий ана-

лог временного ряда $\{z_{ij}\}$, в общем случае нестационарного. Однако если предположить, что характеристики эксперта как некоторой информационно-аналитической оценочной системы остаются неизменными на протяжении процедуры экспертирования, а все ошибки и неточности в экспертных оценках определяются исключительно свойствами и состоянием эксперта на момент проведения экспертизы, то справедливым представляется предположение о стационарности и эргодичности случайных последовательностей $E_j = \{e_{1j}, e_{2j}, ..., e_{Mj}\}$, $j = \overline{1, N}$. В последнем случае для больших значений M оказывается возможным оценивание эмпирических моментных характеристик, эмпирических функций распределения соответствующих погрешностей, и последующее сопоставление этих оценок, найденных для различных экспертов [11, 14, 15]. Можно предположить, что результаты сравнительного анализа будут содержать определенную информацию об уровнях компетентности экспертов. Актуальны проблемы выделения этой информации и ее представление в виде постоянных показателей компетентности, которые допускают достаточно простую интерпретацию. Попытка частичного решения этой проблемы рассмотрена в [7, 8], где по данным сравнительного анализа экспертных оценок выявлялись так называемые «аномальные» эксперты. Оценки, полученные от «аномальных» экспертов, существенно отличаются от оценок, полученных от других экспертов. В частности, это касается формы распределения погрешностей оценок экспертизы и соответствующих моментных характеристик. В целом характер решений, представленных в [7, 8], ближе к методам классификации и не содержит прямых подходов к оценке компетентности экспертов.

Материалы, более адекватные содержанию задач, рассматриваемых в рамках сформулированной выше проблемы, представленные в [8]. Однако предложенный в них уровень описания и формализации задач не позволил получить достаточно общего метода решения, робастного к вариации условий исходной постановки проблемы.

По аналогии с известными положениями кластерного анализа [7, 8] введем понятие образа эксперта как некоторой точки

$Z_j = [z_{1j}, z_{2j}, ..., z_{Mj}]^T$, $j = \overline{1, N}$ в M-мерном пространстве R^M результатов МОЭ. При полном совпадении мнений экспертов их образы совпадают, то есть все результаты экспертизы будут представлены единственной точкой в пространстве результатов МОЭ. Наличие ошибок экспертов приводит к расщеплению точки в облако (кластер), плотность которой (которого) неоднородна и обычно максимальна в области, прилегающей к центру кластера с координатами $Z_0 = [z_{10}, z_{20}, ..., z_{M0}]^T$, определяемыми соотношением [7, 8]:

$$Z_0 = \underset{Z_j, Z_0 \in R^M}{\operatorname{argmin}} \sum_{j=1}^{N} r_j(Z_j, Z_0), \qquad (4.6)$$

где $r_j(Z_j, Z_0)$ – расстояние между образом j-ого эксперта и центром Z_0 кластера в M- мерном пространстве R^M результатов МОЭ. При использовании для нахождения $r_j(Z_j, Z_0)$ евклидовой метрики:

$$r_j = r_j(Z_j, Z_0) = [\sum_{i=1}^{M} (z_{ij} - z_{i0})^2]^{\frac{1}{2}}, \; j = \overline{1, N}, \qquad (4.7)$$

минимизация соотношение (4.6) достигается при:

$$z_{i0} = \frac{1}{N} \sum_{j=1}^{N} z_{ij}.$$

Наличие аномальных данных в строках матрицы Z вызывает смещение среднеарифметических оценок, в связи, с чем более надежный результат (при вероятном наличии «аномальных» экспертов) дает применение робастных медианных оценок вида:

$$z_{i0} = med(Z_i) = med(z_{i1}, z_{i2}, ..., z_{iN}).$$

При отсутствии аномальных экспертов справедливо предположение о равенстве нулю математических ожиданий ошибок экспертизы: $\mu\{E_j\} = 0$, $j = \overline{1, N}$, что приводит к выполнению равенства $\mu\{Z_0\} = X_0 = [x_{10}, x_{20}, ..., x_{M0}]^T$ и позволяет обосновать гипотезу несмещенности среднегрупповых экспертных оценок:

$$\mu\{\bar{Z}_i\} = \mu\{\frac{1}{N} \sum_{j=1}^{N} Z_{ij}\} = \frac{1}{N} \mu\{\sum_{j=1}^{N} x_{i0} + e_{ij})\} = \frac{1}{N} (N x_{i0}) = x_{i0}.$$

Метризация удаленности образов экспертов от центра Z_0 позволяет представить в интегрированной форме информацию об ошибках каждого из экспертов и допускает возможность существования шкального преобразования $c_j = f(r_j)$, что обеспечивает взаимнооднозначное отображения элементов множества R ($r_j \in R$, $j = \overline{1,N}$) в соответствующие оценки компетентности экспертов $f : R \to C$; $c_j \in C$.

Выбор структуры и параметров отображения *f* представляет нетривиальную задачу, которая требует отдельного рассмотрения.

При формировании требований к шкальному преобразованию $c = f(r)$ будем исходить из следующих соображений. Во-первых, очевидно, что с ростом компетентности *C* значение r уменьшаются, то есть производная $dc/dr < 0$. Из этого следует также утверждение о монотонном характере зависимости $c = f(r)$. Во-вторых, при построении шкалы измерения компетентности *C*, множество возможных значений *r*, определенную на полуоткрытом интервале $R = [0,\infty)$, удобно отображать в замкнутый интервал *C* = [1,0], что соответствует типичной шкале компетентности. При этом значению $r \to \infty$ отвечает правое предельная отметка *c* = 0 шкалы компетентности, и значению *r* = 0 – левая, *c* = 1. Для малых значений оценок *r*, учитывая, что величина погрешности оценки в этом случае может быть сопоставим или даже существенно превышать неизвестно истинное значение расстояния *r*, с целью уменьшения влияния погрешности на точность значений компетентности *C*, целесообразно ввести условие:

$$dc/dr \approx 0. \qquad (4.8)$$

При этом для области малых значений *r* будет справедливо соотношение $f(r) = c \approx 1$. Условие, аналогичную (4.8), следует ввести и для области больших значений *r*, которая прилегает к правому концу интервала $R = [0,\infty]$. Тогда точки этой довольно протяженной области больших значений *r* (соответствующие существенно удаленным образам малокомпетентных экспертов от центра Z_0) будут отображаться в значениях компетентности *C*, равные или

близкие 0. В итоге, если предположить, что значение производной dc/dr максимальные (по модулю) в центральной части шкалы и уменьшаются, стремясь к 0, по мере приближения к периферии шкалы, справедливо соотношение:

$$dc/dr = -c(b_0 - b_1 c),\ b_0, b_1 > 0,\ b_0 \geq b_1. \qquad (4.9)$$

Квадратический сдвиг $b_1 c^2$ в правой части (4.9) позволяет реализовать выполнение условия (4.8) в области больших значений *r*. В целом соотношение (4.9) представляет собой дифференциальное уравнение с разделяющимися переменными, решив которое получаем:

$$\ln \frac{c}{b_0 - b_1 c} = -b_0 r + \ln A, \qquad (4.10)$$

где A – постоянная интегрирования. С учетом граничного условия $c(0) = 1$, после потенцирования и ряда преобразований, вводя постоянную $B = b_1 / b_0$, находим:

$$c = f(r) = \frac{1}{(1 - \frac{b_1}{b_0})e^{b_0 r} + \frac{b_1}{b_0}} = \frac{1}{(1-B)e^{b_0 r} + B}. \qquad (4.11)$$

График зависимости *c*(*r*), приведен на рис. 4.1, по своему характеру – «перевернутая» логистическая кривая.

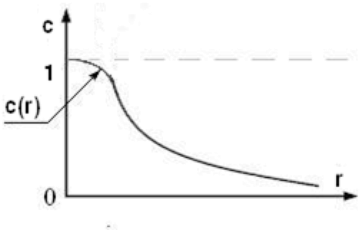


Рис. 4.1. График зависимости *c*(*r*)

Полученные выше результаты, к сожалению, носят сугубо прикладной характер. Рассчитанные по формуле (4.7) оценки *r* позволяют сопоставлять уровни ошибок экспертов только в рамках конкретной задачи. Это объясняется тем, что найденные оценки *r* зависят от числа объектов экспертизы *M* и количественных характе-

ристик принятой шкалы оценок. Полученная на базе достаточно общих и объективных предпосылок структура шкального преобразования $c = f(r)$ для своей конкретизации и прикладного применения требует задания количественных значений параметров b_0, B, что становится возможным только при определении конкретного типа экспертизы.

Поэтому далее, для получения возможности более детального учета особенностей и характера МОЭ, немного сузим класс исследуемых процедур экспертизы. Рассмотрим достаточно распространенную на практике процедуру МОЭ, в которой используется балльное оценивание.

Если процедура МОЭ заключается в оценке каждого из объектов экспертизы в бальной шкале $0,1,2,...,l_{\max}$, то есть $z_{ij} \in \{0,1,...,l_{\max}\} = L$, то теоретически возможными минимальными и максимальными значениями r будут $r_{\min} = 0$ и $r_{\max} = l_{\max}\sqrt{M}$. Вводя в выражение (4.7) нормирующие множители $1/l_{\max}$ и $1/\sqrt{M}$, получаем формулу для вычисления нормированного удаления (расстояния) образа *j*-ого эксперта от центра кластера Z_0:

$$r_{нj} = r_j / (l_{\max}\sqrt{M}).$$

Нормированное расстояние не зависит от числа М объектов, подлежащих экспертизе, и количества отсчетов балльной шкалы, то есть от $l_{\max}$, и, будучи индивидуализированной оценке эксперта, учитывает только величину и характеристики распределения ошибок эксперта. Типичное распределение совокупности значений $r_н$ для группы экспертов представлено на рис. 4.2.

Опыт практической работы с данными МОЭ свидетельствует, что значения $r_н \le 0,2$ характерны для экспертов достаточно высокой квалификации, значения $r_н \ge 0,3 \div 0,35$ свидетельствуют о присутствии аномальных данных в оценках эксперта, область значений $0,2 < r_н < 0,3 \div 0,35$ соответствует образам экспертов, имеющим относительно невысокий уровень профессиональной подготовки,

неровно проводящих экспертизу и допускающих в своих оценках ошибки довольно значительной величины.

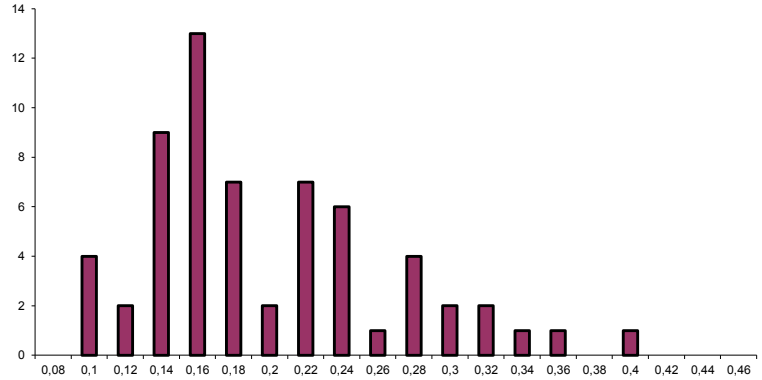


Рис. 4.2 Типичное распределение совокупности $r_н$ для группы экспертов

В частности, подобную характеристику шкальному превращению обеспечивают следующие значения параметров: b_0=15, B=0,967 (рис. 4.3). Следует отметить, что в этом случае непосредственное выявление и исключение из обработки данных «аномальных» экспертов отсутствует. Это объясняется тем, что при осуществлении обработки с введением весов, пропорциональных компетентности экспертов, данные, полученные от экспертов, для которых $r_н$ >0,4, фактически обнуляются.

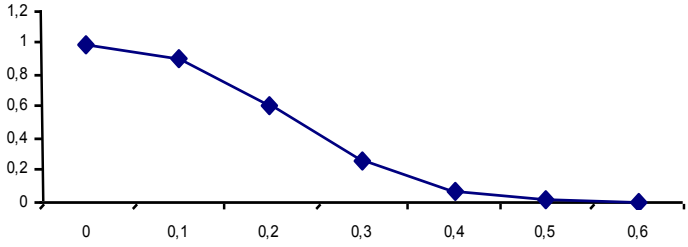


Рис. 4.3. График характеристики шкального преобразования (4.11) с параметрами: b_0=15, B=0,967

Очевидно, что задание параметров шкального преобразования содержит существенный субъективный момент и определяется целями преобразования, особенностями принятой модели распределения погрешностей оценок экспертизы, применяемым способом количественного оценивания уровня компетентности (балльная шкала, шкала с односторонним ограничением, шкала с двусторонним ограничением и т.п.).

Поставив в соответствие элементам вектора $Z_j = [z_{1j}, z_{2j}, ..., z_{Mj}]^T$, представляющего результаты M экспертиз, проведенных j-им экспертом, последовательность целочисленных моментов времени $t_i = 1, 2, ..., M$, получим некий аналог временного ряда $\{z_{ij}\}$, в общем случае нестационарного. Однако, если предположить, что характеристики эксперта как некоторой информационно-аналитической системы оценки, остаются неизменными на протяжении процедуры экспертирования, а все ошибки, ошибки и неточности в экспертных оценках определяются исключительно индивидуальными свойствами эксперта при проведении экспертизы, то правильным кажется предположение стационарности и эргодичности случайных последовательностей $E_j = \{e_{1j}, e_{2j}, ..., e_{Mj}\}$, $j = \overline{1, N}$. В этом случае при больших значениях M оказывается возможным оценивания эмпирических моментных характеристик и эмпирических функций распределения соответствующих погрешностей E_j, дальнейший анализ и сопоставление этих оценок, найденных для различных экспертов, с целью выявления в них определенных общих тенденций и закономерностей [7, 8, 11]. Предполагается, что указанные сведения и данные содержат информацию об уровнях компетентности экспертов. Так же актуальна проблема выделения этой информации и ее представления (объяснение) через систему количественных показателей, которые достаточно полно и всесторонне характеризуют качество работы эксперта, легко вычисляются по данным экспертизы и имеют относительно прозрачную интерпретацию.

Методология решения этой проблемы представлена в [7, 8, 11], где для совокупности экспертов было предложено рассчитать

оценки их компетентности c_j, $j=\overline{1,N}$, по данным, полученным путем обработки соответствующих персональных последовательностей $E_j=\{e_{1j},e_{2j},...,e_{Mj}\}$. В частности, такими данными могут быть оценки моментных характеристик μ_{1j}, μ_{2j}, μ_{02j},…, которые затем будут использоваться для построения аппроксимативных модели компетентности $c(\mu_{1j},\mu_{2j},\mu_{02j})$.

Детализация этой методики предполагает следующие действия.

Для совокупности экспертов по имеющимся результатам МОЭ рассчитываются индивидуальные оценки компетенций c_j, $j=\overline{1,N}$, образующих вектор значений моделируемой переменной C. При этом по данным МОЭ сначала определяются значения расстояний r_{ij}, $j=\overline{1,N}$, из которых путем пересчета по формуле

$$c=f(r_{и})=(0,033e^{15r_{и}}+0,967)^{-1},$$

что получена из общего соотношения (4.10) после подстановки в него параметров $b_0=15$, $B=0,967$, формируются соответствующие элементы вектора C. Моментные характеристики последовательностей $E_j=\{e_{1j},e_{2j},...,e_{Mj}\}$, которые индивидуально характеризуют действия каждого из экспертов, рассчитываются по формулам:

- среднее отклонений оценок j-того эксперта

$$\mu_{1j}=\frac{1}{M}\sum_{i=1}^{M}\delta_{ij},$$

- выборочный второй начальный момент

$$\mu_{2j}=\frac{1}{M}\sum_{i=1}^{M}\delta_{ij}{}^{2},$$

- выборочная дисперсия

$$\mu_{02j}{}^{2}=\frac{1}{M-1}\sum_{i=1}^{M}\left(\delta_{ij}-\mu_{1j}\right)^{2},$$

где $\delta_{ij}=z_{ij}-z_{i0}$ – оценки случайных погрешностей e_{ij}, $i=\overline{1,M}$, определяемых в процессе обработки результатов МОЭ.

Вся совокупность моментных характеристики погрешностей оценок экспертов образует матрицу $X=[\mu_{1j},\mu_{2j},\mu_{02j}]$, $j=\overline{1,N}$, моментные характеристики *j*-го эксперта составляют ее *j*-ю строчку. Сведение вместе вектора C и матрицы X позволяет построить модель компетентности $c(\mu_{1j},\mu_{2j},\mu_{02j})$. В частности, считая, что модель относится к классу линейных регрессионных моделей, на базе расширенной матрицы данных $[C,X]$, применяя методы и приемы регрессионного анализа (например, шаговую регрессию для подбора структуры регрессии и метод наименьших квадратов для вычисления регрессионных коэффициентов), получаем аппроксимативных модель вида:

$$c(\mu_1,\mu_2,\mu_{02})=1-11,6\mu_2+50\mu_1^{\,2}\mu_2+40\mu_{02}^2. \quad (4.12)$$

Выражение (4.12) дает возможность количественно оценить уровни компетентности каждого из экспертов, участвовавших в МОЕ, не прибегая к предварительному вычисления нормированной расстояния.

Ниже в таблице 4.1 приведен фрагмент матрицы исходных данных, а также значение нормированного расстояния $r_{нj}$ и модельные значения компетенций $c(x_{1j},x_{2j},x_{3j})$, найденные по формуле (4.12).

Табл. 4.1. Фрагмент матрицы исходных данных

№	$r_{нj}$	$c_j=f(r_{нj})$	$c(x_{1j},x_{2j},x_{3j})$	x_{1j}	x_{2j}	x_{3j}
1	0,402	0,07	0,05	-0,296	0,0741	0,1616
2	0,300	0,25	0,24	-0,197	0,0510	0,0899
3	0,291	0,28	0,27	-0,137	0,0657	0,0845
4	0,256	0,40	0,41	-0,049	0,0633	0,0656
5	0,246	0,44	0,45	0,217	0,0136	0,0605
6	0,206	0,59	0,57	0,166	0,0152	0,0426
7	0,184	0,67	0,65	-0,032	0,0330	0,0340
8	0,137	0,81	0,80	0,031	0,0177	0,0186
9	0,110	0,88	0,87	-0,009	0,0120	0,0121
10	0,097	0,90	0,90	0,008	0,0093	0,0093

Отметим, что при использовании формулы (4.12) не накладывается никаких ограничений на способ нахождения значений моментных характеристик, единственным регламентирующим требо-

ванием является определение экспертных оценок путем применения процедуры балльного оценивания. Соответственно, это означает возможность применения формулы (4.12) для оценки компетентности экспертов, участвующих в любых экспертизах (не обязательно МОЭ), где применяются балльные оценки.

Казалось бы, что для обеспечения удобства практического применения (принимая во внимание, что $\mu_2 = \mu^2{}_1 + \mu_{02}$) формулу (4.12) целесообразно представить как двухфакторную зависимость $c(\mu_{1j}, \mu_{02j})$. Однако при построении модели $c(\mu_{1j}, \mu_{2j}, \mu_{02j})$ по реальным данным при выборе ее структуры именно регрессоры $\mu_2, \mu_1{}^2\mu_2$ оказались базовыми, тогда как начальный момент μ_{02} было введено в структуру модели только при ее окончательной настройке, то есть в принципе возможно применение упрощенной двухфакторной модели вида:

$$c(\mu_1, \mu_2) = 1 - 10{,}7\mu_2 + 54\mu_1{}^2\mu_2 . \qquad (4.13)$$

Наличие в формулах (4.12), (4.13) синергетического регрессора $\mu_1{}^2\mu_2$ приводит к определенным трудностям в случае невозможности объективного задания значения момента μ_1 и попытки решить эту проблему введением оценки μ_1=0. В этой ситуации лучшие результаты дает применение модели

$$c(\mu_2) = 1 - 9{,}6\mu_2 .$$

В общем, суммируя материалы, приведенные в данном разделе, приходим к следующему выводу: вероятность существенных субъективных ошибок в индивидуальных (персональных) экспертных оценках требует в случае использования этих оценок для принятия важных решений опираться на результаты групповых (коллективных) экспертиз, что в свою очередь обусловливает необходимость разработки специальных методик обработки данных групповых экспертиз. Подавляющее большинство этих методик базируется на использовании дополнительной информации об индивидуальном уровне компетентности экспертов, задействованных в экспертизах, в связи с чем возникает потребность в проведении вспомогательных организационных мероприятий для получения данных об уровнях компетентности экспертов.

Однако в случае так называемой многообъектной экспертизы, требованиям которой соответствуют формы работы большинства экспертных комиссий, необходимые сведения о компетентности экспертов становится возможным получить непосредственно из данных групповой экспертизы. Это существенно упрощает и ускоряет проведение организационных процедур групповой экспертизы.

СПИСОК ЛИТЕРАТУРЫ К ГЛАВЕ 4

1. С.О. Носок, *Методи обробки експертних даних в задачі автоматизації профвідбору. Дисертація на здобуття наукового ступеня канд. техн. наук*., К., 2007, с. 160.
2. «Про державну таємницю», *Закон України,* станом на 13 жовтня 2010 року, режим доступу: http://zakon1.rada.gov.ua.
3. «Положення про експертні комісії з питань державної таємниці». *Наказ Служби безпеки України від 04.01.2005р. № 696*, Офіційний Вісник України, № 2, Ст. 107, 2005.
4. «Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності», *Державний комітет України з питань державних секретів та технічного захисту інформації*; Збірка №8, Наказ № 23 від 9 лютого 1998, К., С.4-14, 1998.
5. О.Є. Архипов, І.П. Касперський, «Проблеми методичного забезпечення віднесення відомостей до інформації з обмеженим доступом в Україні», *Правова інформатика*, №3 (11), С.61-66, 2006.
6. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Технологии экспертного оценивания в задачах защиты информации», *Інформаційні технології та комп'ютерна інженерія*, № 2, С.89–94, 2005.
7. А.Е. Архипов, С.А. Архипова, С.А. Носок, И.В. Пишко, «Применение методов кластеризации в задаче обработки данных экспертного опроса», *Радіоелектроніка, інформатика, управління*, № 2(10), С.104–108, 2003.
8. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Применение кластерного анализа для структурирования данных экспертного опроса», *Адаптивные системы автоматического управления*, №6(26), С.55–61, 2003.
9. А.Н. Ефимов, *Информация: ценность, старение, рассеяние*, М., Знание, 1978,с. 64.
10. С.А. Петренко, С.В. Симонов, *Управление информационными рисками. Экономически оправданная безопасность*. М., Компания Ай Ти; ДМК Пресс, 2004, с. 348.

11. А.Е. Архипов, С.А. Архипова, *Математичне моделювання соціальних систем і процесів: Навч.-метод. посіб*., К., ІВЦ «Видавництво «Політехніка», 2002, с. 60.

12. О.Є. Архипов, О.Є. Муратов, *Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія*, К., Наук.-вид. відділ НА СБ України, 2011, с. 195.

13. О.Є. Архипов, С.А. Архіпова, «Оцінювання якості роботи експертів за даними багатооб'єктної експертизи», *Захист інформації*, №4 (53), С.45 – 54, 2011.

14. А.Е. Архипов, С.А. Архипова, С.А. Носок, «О построении модели компетентности эксперта», *Системні технології. Системи управління, контролю та технічної діагностики: Зб. наук. праць*., Вип.8, Дніпропетровськ: «Системні технології», С.22-25, 2006.

15. А.Е. Архипов, С.А. Архипова, С.А. Носок, «Модели компетентности эксперта», *Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій* (ISMIT'2006), м. Євпаторія, 15-19 травня 2006р., том 1, С. 22-25, 2006.

Научное издание

Рекомендовано Ученым советом Каспийского государственного университета технологий и инжиниринга имени Ш.Есенова

Авторы

Б.Б. Ахметов, А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук

ПОСТРОЕНИЕ СИСТЕМ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ТЕОРИЯ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ
(Книга 1)

Подписано в печать 08.10.2018 г.
Формат 60x84 1/16
Печать лазерная. Гарнитура «Times New»
Усл. печ.л. 33 Тираж 500 экз.
Цена договорная

Отпечатано в редакционно-издательском отделе
КГУТИ им. Ш. Есенова
Адрес: 130000, Республика Казахстан,
г. Актау, 32 мкрн.