ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59503— 2021/ISO/IEC TR 27016:2014

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Экономика информационной безопасности организации

(ISO/IEC TR 27016:2014, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 386-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TR 27016:2014 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации» (ISO/IEC TR 27016:2014 «Information technology — Security techniques — Information security management — Organizational economics», IDT).

ISO/IEC TR 27016 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного документа, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В настоящем стандарте содержатся рекомендации по экономическому обеспечению информационной безопасности (ИБ) в виде процесса принятия решений, касающихся производства, распространения и потребления товаров и услуг, имеющих ограничения. Для принятия мер по защите информационных активов организации требуются ресурсы, которые в ином случае могли бы быть выделены на другие цели, не относящиеся к ИБ. Настоящий стандарт предназначен преимущественно для исполнительного руководства, выполняющего решения административного органа по стратегии и политике, например генеральных директоров (CEO), глав правительственных организаций, финансовых директоров (CFO), главных операционных директоров (COO), директоров по информационным технологиям (CIO), директоров по ИБ (CISO) и прочих лиц, выполняющих схожие обязанности[1)].

Менеджмент ИБ часто рассматривается как комплекс мер в области информационных технологий с использованием технических средств управления (например, шифрования, межсетевых экранов, инструментов нейтрализации вторжений и вредоносного кода). Однако никакие меры по обеспечению ИБ не будут эффективны без использования широкого спектра других средств управления (т. е. физических средств управления, средств управления персоналом, политик, правил и т. п.). Для реализации всего этого спектра средств управления в рамках менеджмента ИБ необходимы решения о выделении достаточных ресурсов. В этом техническом отчете излагаются сведения, необходимые для решения задач ИБ в соответствии с комплексом стандартов ИСО/МЭК 27000. Подход заключается во внедрении экономической модели как ключевого элемента процесса принятия решений.

Наряду с методикой менеджмента рисков (см. ИСО/МЭК 27005) и возможностью измерения параметров ИБ (см. ИСО/МЭК 27004), экономические факторы следует рассматривать в контексте менеджмента ИБ в процессе планирования, развертывания, обслуживания и улучшения системы безопасности информационных активов организации. В частности, эффективное расходование средств на информационную безопасность невозможно без экономического обоснования.

Как правило, экономические преимущества менеджмента ИБ полностью или частично заключаются в следующем:

a) сведение к минимуму любого отрицательного воздействия на коммерческие задачи организации;

b) ограничение любых финансовых потерь приемлемым уровнем;

c) отсутствие необходимости в выделении дополнительных средств на покрытие рисков или непредвиденных расходов.

Менеджмент ИБ также может обеспечить преимущества, не связанные напрямую с материальными вопросами. Такие нематериальные преимущества немаловажны, но обычно остаются вне рамок финансово-экономического анализа. Преимущества подобного характера должны получить количественную оценку и стать частью экономического анализа. Примерами преимуществ являются:

a) возможность для организации участвовать в проектах, сопряженных с повышенным риском;

b) возможность для организации обеспечивать соблюдение законодательных и нормативных требований;

c) возможность для организации соответствовать ожиданиям потребителей;

d) возможность для организации соответствовать ожиданиям сообществ;

e) повышение репутации и доверия к организации;

f) гарантии полноты и точности финансовой отчетности.

Все более острой проблемой организаций становятся отрицательные финансовые и нефинансовые воздействия, являющиеся результатом ее неспособности обеспечить надежную защиту своих информационных активов. Среди прочих ценных аспектов менеджмента ИБ можно указать выявление прямой зависимости между затратами на средства управления, призванные предотвратить потери, и достигаемой благодаря этому экономией.

Ужесточение конкуренции вынуждает организации сосредоточиться на экономической подоплеке рисков.

Настоящий стандарт представляет собой дополнение к комплексу стандартов ИСО/МЭК 27000, обосновывающее экономический подход к защите информационных активов организации в контексте расширенной общественной и социальной среды ее деятельности.

[1)] *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент информационной безопасности. Экономика информационной безопасности организации

Information technology. Security techniques. Information security management. Organizational economics

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит рекомендации по принятию организациями решений, связанных с защитой информации, и учету экономических последствий таких решений в контексте неоднозначных требований к ресурсам.

Настоящий стандарт применим к организациям любого типа и масштаба деятельности и включает в себя информацию, необходимую для принятия экономических решений в сфере менеджмента ИБ высшим руководством.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения).

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Общий обзор и терминология)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями:

3.1 **ожидаемые потери в годовом исчислении;** ALE (annualized loss expectancy, ALE): Ожидаемые материальные потери (3.13), связанные с активом, из-за актуальных рисков в течение года.

Примечание — Показатель ALE рассчитывается следующим образом: ALE = SLE · ARO, где SLE — потенциальный ущерб от реализации единичной угрозы, ARO — ожидаемая годовая частота реализации угрозы.

3.2 **прямая ценность** (direct value): Ценность, определяемая ценностью идентичной замены или замещения в случае повреждения либо потери информационного актива.

Примечание — Этот показатель имеет положительное значение при отсутствии повреждения актива, однако рассматривается как потеря при наступлении соответствующего события.

3.3 **экономический фактор** (economic factor): Компонент или информация, влияющие на стоимость актива.

3.4 **экономическое сравнение** (economic comparison): Анализ взаимоисключающих или альтернативных вариантов распределения ресурсов.

Издание официальное

3.5 **экономическое обоснование** (economic justification): Элементы экономической модели, создаваемые для поддержки выделения ресурсов.

3.6 **добавленная экономическая ценность** (economic value added): Индикатор сравнения чистой операционной прибыли и общей стоимости капитала.

3.7 **экономика** (economics): Эффективное использование ограниченных ресурсов.

3.8 **ожидаемый убыток** (expected value): Потеря стоимости на предприятии, связанная с повреждением или потерей информационного актива.

Примечание — Этот показатель имеет положительное значение при отсутствии повреждения актива, однако рассматривается как потеря при наступлении соответствующего события.

3.9 **расширенный убыток** (extented value): Ожидаемый убыток, помноженный на количество раз его возникновения.

3.10 **косвенный убыток** (indirect value): Потеря стоимости, связанная с затратами на замену или восстановление информационного(ых) актива(ов) в случае его (их) повреждения или потери.

Примечание — Этот показатель имеет положительное значение при отсутствии повреждения актива, однако рассматривается как отрицательный при наступлении соответствующего события.

3.11 **экономическая модель информационной безопасности** (information security economics): Эффективное использование ограниченных ресурсов для управления информационной безопасностью.

3.12 **менеджмент информационной безопасности;** ISM (information security management, ISM): Управление аспектами сохранения конфиденциальности, целостности и доступности информации.

3.13 **потеря** (loss): Уменьшение ценности актива.

Примечание — В контексте экономической модели информационной безопасности (3.11) потери выражаются положительными значениями. В настоящем стандарте понятие стоимости всегда имеет отрицательное значение при отсутствии указания на обратное.

3.14 **рыночная стоимость** (market value): Наивысшая цена, которую готов уплатить подготовленный, готовый к покупке и дееспособный покупатель и наименьшая цена, приемлемая для продавца.

3.15 **чистая стоимость** (net present value): Сумма показателей текущей стоимости (3.16) отдельных денежных потоков одного предприятия.

3.16 **текущая стоимость** (present value): Оцениваемая в данный момент сумма денежных средств или их потоков с учетом указанного коэффициента окупаемости.

3.17 **неэкономическое преимущество** (non economic benefit): Преимущество, за которое не производится оплата.

3.18 **стоимость возможности** (opportunity cost): Расчетная будущая стоимость определенного(ых) мероприятия(й) по обеспечению ИБ.

3.19 **ценность возможности** (opportunity value): Расчетная будущая выгода от определенного(ых) мероприятия(й) по обеспечению ИБ.

3.20 **нормативные требования** (regulatory requirements): Обязательные требования к ресурсам, связанные с определенным рынком.

3.21 **коэффициент окупаемости инвестиций** (return on investment): Уровень доходности (или убыточности) с учетом суммы вложенных в экономическую единицу средств за определенный период.

3.22 **общественно-значимые ценности** (societal value): Общепринятое представление о плохом и хорошем.

3.23 **ценность** (value): Относительная стоимость актива по сравнению с другими объектами или определенным абсолютным значением.

Примечание — Этот показатель может быть положительным или отрицательным в контексте экономической модели информационной безопасности (3.11). В настоящем стандарте понятие ценности всегда имеет положительное значение при отсутствии указания на обратное.

3.24 **ценность под угрозой;** VAR (value-at-risk, VAR): Максимальная сумма потерь (3.13) в наихудшем случае в течение данного периода времени и с заданной вероятностью.

Примечание — Период времени может составлять, например, один год, а заданную вероятность также называют степенью уверенности.

4 Обозначения и сокращения

BVM — модель базовой стоимости;
CIA — конфиденциальность, целостность, доступность;
IRP — паритет процентных ставок;
ROI — коэффициент окупаемости инвестиций;
ИКТ — информационно-коммуникационные технологии;
СМИБ — система менеджмента информационной безопасности.

5 Структура настоящего стандарта

Фундаментальным фактором организационной экономики модели менеджмента ИБ является обеспечение экономических показателей для руководства. Это позволяет принимать более взвешенные решения в отношении того, какие ресурсы могут быть направлены на защиту информационных активов организации.

В разделе 6 приводится описание экономических факторов ИБ и их влияния на принятие управленческих решений. В разделе 7 описываются экономические задачи в контексте оценки активов. В разделе 8 излагаются принципы обеспечения экономического равновесия между преимуществами и издержками ИБ в общем организационном контексте с примерами в зависимости от категории бизнес-модели.

Упомянутые выше разделы снабжены следующими приложениями:

- в приложении А приведен широкий спектр задач заинтересованных сторон в отношении ценностных аспектов ИБ;
- в приложении В изложены коммерческие задачи, а также вопросы издержек организаций, связанных с ИБ;
- в приложении С содержится набор моделей, которые могут использоваться для организационной экономики ИБ;
- в приложении D приводятся примеры использования моделей с примерными показателями.

6 Экономические факторы информационной безопасности

6.1 Управленческие решения

Комплекс стандартов ИСО/МЭК 27000 описывает целый спектр коммерческих задач, требующих принятия управленческих решений. С их помощью организации в официальном или неформальном порядке оценивают собственные потребности во вложениях в системы ИБ. Качество таких управленческих решений можно значительно повысить, если проектировать соответствующие процессы, сравнивая чистую отдачу от вложений в системы ИБ с потребностями в ресурсах в других сферах деятельности организации.

Процесс принятия решений в области ИБ должен иметь четкую основу, учитывающую соответствующие факторы, связанные с экономикой ИБ организации. Экономическая ценность вложений в ИБ должна определяться с учетом коммерческих задач организации. Наличие прямой увязки коммерческих задач между собой дает возможность вводить другие факторы, такие как риски, затраты и преимущества, чтобы повысить эффективность измерений.

Руководству также необходимо учитывать надлежащее экономическое обоснование для выделения ресурсов на обеспечение ИБ активов, что должно допускать возможность экономического сравнения с другими вариантами использования ресурсов. Одним из принципов является применение подхода к выделению ресурсов (например, чистая стоимость, окупаемость инвестиций, добавленная экономическая ценность) в рамках программы менеджмента ИБ с целью получения результатов, сравнимых с задачами принятия решений, с учетом следующих аспектов:

а) некоторые преимущества программы менеджмента ИБ могут иметь неэкономический характер ввиду сложности объективной и последовательной оценки таких преимуществ по экономической шкале. Например, наличие нормативных требований к защите или предоставлению определенной информации может делать невозможным определение экономической ценности соответствующего преимущества. Подобная ситуация также рассматривается как стоимость выполнения требований;

b) аналогичным образом, невозможно в терминах экономических показателей получить объективную оценку общественно-значимой ценности внедрения программы менеджмента ИБ без эффективного механизма обратной связи от сообщества. Неэкономические преимущества являются важным фактором в обосновании программы менеджмента ИБ. Однако их невозможно определить методами экономического анализа из-за сложностей с последовательной оценкой таких преимуществ;

c) меры ИБ могут применяться для защиты нематериальных активов, таких как бренд, репутация и т. п. Масштабы подобной защиты необходимо рассчитывать и представлять в связке с методами оценки таких нематериальных активов, применяемыми организацией. Экономические аспекты оценки следует увязывать с эффектом от применения мер ИБ в отношении нематериального актива. Экономические показатели должны предоставляться отделами организации, например финансовым отделом, отделом управления рисками, отделами продаж, маркетинга и т. д. Расчет затрат на меры по защите должен производиться исходя из уровня ИБ.

6.2 Технико-экономическое обоснование

Технико-экономическое обоснование инвестиций в системы ИБ дает организации возможность понять, превышают ли экономические преимущества объем требуемых затрат и, если превышают, то насколько. В тех случаях, когда задачи ИБ предлагаются на рассмотрение руководству организации (как правило, в виде технико-экономического обоснования), должны быть учтены экономические аспекты. В коммерческом предложении должны учитываться затраты, связанные с обеспечением ИБ. Например, каким будет экономическое воздействие реализации (нереализации) определенной меры на возможность решения стоящих перед организацией задач. Технико-экономическое обоснование должно давать четкий ответ на этот вопрос.

В технико-экономическом обосновании должна содержаться взвешенная оценка затрат, выгод и рисков. Это необходимо для того, чтобы организация могла учесть все варианты и последствия, связанные с каким-либо решением, а также определить важность конкретной инвестиции в безопасность для достижения наилучших результатов. Такие последствия и варианты могут иметь положительный характер, если объем инвестиций определен правильно, либо отрицательный характер, если инвестиции окажутся недостаточными.

Технико-экономическое обоснование следует рассматривать в контексте инвестиционных затрат на обеспечение ИБ в сравнении со всеми издержками, сопряженными с рисками. Основополагающие элементы технико-экономического обоснования должны предоставлять достаточно информации для принятия решений, в частности:

a) стоимость информационного актива;
b) потенциальные риски, связанные с информационным активом;
c) известная стоимость обеспечения защиты информационного актива;
d) степень снижения риска в связи с принимаемой мерой.

В определенной точке стоимость мер по защите информационного актива станет оптимальной. Оптимальная стоимость издержек по защите актива достигается в тех условиях, когда снижение риска, влияющее на стоимость, окажется меньше стоимости реализации меры по защите (см. также приложение С, модель С.4).

Рисунок 1 демонстрирует необходимость учета экономических факторов коммерческих процессов в рамках технико-экономического обоснования.

При подготовке технико-экономического обоснования и определении приоритетов организация должна учитывать неизменную конечность ресурсов, а таюке собственные потребности. Аспекты ИБ должны основываться на фактах и достоверных данных по мере их наличия. Расчеты необходимо выполнять с учетом всех имеющихся сведений и опыта, в частности:

e) расчеты по временным отрезкам (максимальный, минимальный период и т. д.);
f) сметы затрат;
g) котировки;
h) прогнозирование рыночной стоимости;
i) известные или ожидаемые сборы и штрафы за несоответствие требованиям;
j) юридические последствия в прямой и косвенной формах;
k) оценки риска с прогнозами возможных потерь;
l) ценность возможностей;
m) стоимость возможностей.

Рисунок 1 — Процесс принятия решений организационно-экономического характера в отношении ИБ с помощью настоящего стандарта

Прогнозы по временным периодам должны формироваться на базе статистики, оценок рисков и т. п. При определении временных периодов имеет смысл проконсультироваться с экспертами из всех задействованных отделов и подразделений.

В экономические аспекты менеджмента ИБ должно входить следующее:

n) действия и решения в течение всего процесса менеджмента ИБ;

o) экономические обоснования принятия решений о годовых инвестициях в связи с процессом менеджмента ИБ;

p) обеспечение соответствия процесса менеджмента ИБ требованиям ИСО/МЭК 27001 (СМИБ).

Сложность технико-экономического обоснования (ТЭО) менеджмента ИБ зависит от сферы применения, которая, в свою очередь, учитывает среду реализации средств ИБ. Чтобы отразить экономические аспекты системы ИБ в технико-экономическом обосновании, необходимо увязывать коммерческие факторы обоснования с фактическим решением по обеспечению ИБ. На различных уровнях организации к технико-экономическому обоснованию применяются разные экономические модели. Такие уровни можно разделить на две категории: Категория А — организационный уровень, категория В — процессы, функции и т. п. Организационный уровень может включать в себя разнообразные активы. С точки зрения менеджмента ИБ, категория В может также являться областью применения технико-экономического обоснования в отношении средства (средств) управления.

Таблица 1 — Распределение ТЭО по категориям

Категория технико-экономического обоснования (ТЭО)	Тип и область применения	Описание типа ТЭО	Пример СМИБ	Характеристики расчета
A	Организация в целом	Более высокий и более концептуальный уровень ТЭО описывает меры по обеспечению ИБ, применяемые в рамках всей организации или ее большей части	Стандартные случаи: внедрение СМИБ, слияние с другой организацией или ее приобретение. Предполагается, что внедрение СМИБ во всей организации происходит в согласованных границах области применения	Общие расчеты ценности возможностей организации и затрат на реализацию и применение положений ТЭО. Разброс показателей ценности и затрат рекомендуется ограничить определенным диапазоном

Окончание таблицы 1

Категория технико-экономического обоснования (ТЭО)	Тип и область применения	Описание типа ТЭО	Пример СМИБ	Характеристики расчета
B	Часть организации, такая как процесс/отдел/и (или) функциональные подразделения	Обоснование исходя из вида деятельности или меры по обеспечению ИБ	Стандартный случай: аутсорсинг ИКТ, компьютерный центр	Может быть несколько вычислений, и результаты, возможно, потребуется объединить. Расчет стоимости и затрат, как правило, легко определить, но может потребоваться оценка для сложных бизнес-кейсов. Диапазон рекомендуется использовать для оценки значений, но не затрат

В приложении В содержится дополнительная информация об экономических решениях и учитываемых при их принятии ключевых факторах.

6.3 Заинтересованные стороны

Согласно ИСО/МЭК 27001, СМИБ должна использоваться на благо заинтересованных сторон. Продвижение их интересов должно учитывать экономические аспекты ИБ. В тех случаях, когда реализация мер по обеспечению ИБ может отрицательно воздействовать на заинтересованные стороны, необходимо учесть экономические факторы. Для примера можно привести следующие типы ценности:

a) общественно-значимая ценность (например, нужно ли учитывать общую материальную ценность для определенного круга общества либо следует задать какие-либо ограничения);

b) ценность бренда, ценность основного направления бизнеса и т. д.;

c) репутация;

d) ценность для потребителей;

e) права интеллектуальной собственности;

f) в зависимости от типа деятельности (например, в секторе здравоохранения, транспорта и т. д.), может потребоваться учет специфических видов материальной ценности.

Возможно, что другие отделы организации уже учли эти типы ценности в собственных экономических расчетах и могут внести свой вклад в рассмотрение вопросов ИБ.

В приложении А приводится дополнительная информация о заинтересованных сторонах и их целях.

6.4 Проверка экономических решений

Для реализации и текущего менеджмента средств управления ИБ в целях защиты информационных активов требуются ограниченные ресурсы организации. В этой связи такие ресурсы следует рассматривать как элемент ценности, способный принести ощутимую отдачу в будущем (например, способный предотвратить кражу секретной информации).

В ИСО/МЭК 27004 указывается, что организация должна регулярно оценивать, насколько применяемые меры по обеспечению ИБ позволяют ей достичь своих целей. Процесс такой оценки применим и к анализу экономических инвестиций организации в ограниченный перечень товаров и услуг. Например, позволяет определить, насколько обоснованными являются следующие типы затрат:

a) затраты на реализацию процессов и проектов по оценке рисков;

b) затраты на организационную инфраструктуру, в том числе на сотрудников, обеспечивающих ИБ;

c) затраты на средства управления ИБ (например, затраты на решения для контроля доступа пользователей, затраты на шифрование резервных копий), обеспечивающие надлежащий и неизменный уровень защиты в соответствии с готовностью организации к рискам (например, приемлемый уровень остаточного риска);

d) затраты на применение мер по обеспечению непрерывного тестирования, гарантированной эффективности процессов и (или) сертификации на предмет соответствия систем ИБ определенному стандарту;

e) затраты на формирование соответствующей культуры, обучение и повышение уровня осведомленности в целях уменьшения числа инцидентов в сфере ИБ.

Примечание — Инвестиции в организационную инфраструктуру и обучение могут иметь менее выраженный на первоначальном этапе, но более продолжительный эффект. Таким образом, для оценки их эффективности следует использовать более длительный отрезок времени.

7 Экономические задачи

7.1 Введение

Для того, чтобы применить экономическую модель к менеджменту ИБ, требуется соответствующая информация, содержащаяся в политике менеджмента ИБ. На ее основе работают все механизмы принятия экономических решений организации. Этот процесс достаточно просто применять в отношении финансово-экономических аспектов, однако он может вызывать затруднения при оценке аспектов, не связанных с финансами.

Экономические решения подразумевают расстановку приоритетов в отношении ограниченных ресурсов товаров и услуг с целью оптимизации решения организационных задач. Такие экономические решения в равной степени относятся как к менеджменту ИБ, так и к другим элементам структуры организации.

В приложении В приведены примеры факторов ИБ, определяющих оптимальное решение нескольких задач. Каждое решение, связанное с затратами, может влиять на достижение результатов в области ИБ. Например, увеличение вложений в нейтрализацию рисков позволяет организации работать в более безопасной среде, но может препятствовать оперативному реагированию на происходящие перемены.

7.2 Оценка информационных активов

Оценка информационных активов для целей ИБ должна осуществляться с учетом критериев конфиденциальности, целостности и доступности (и любых других аспектов ИБ, предусматриваемых в данной организации). Определяемая денежная ценность актива должна отражать последствия для деятельности организации в случае ухудшения фактических критериев его оценки. Например, нарушение целостности общедоступного веб-сайта (т. е. появление на нем вводящей в заблуждение информации) может иметь последствия для деятельности его владельца, выражаемые в денежном эквиваленте. Денежная ценность такого веб-сайта с точки зрения конфиденциальности равна нулю, поскольку информация является общедоступной. Если такой веб-сайт станет недоступен, последствия для деятельности его владельца в денежном выражении будут иными, поскольку внешние пользователи не смогут посещать данный сайт. Таким образом, существует три различных значения ценности (с учетом приведенных выше критериев) для данного актива. Это руководство следует учитывать при проведении оценки активов.

Поскольку оценка нематериальных активов может вызывать затруднения, существуют два простых метода: использование простой сравнительной шкалы (например, низкий, средний, высокий уровень) и числовой шкалы (например, 1—4). Эти методы особенно подходят для тех случаев, когда значения и (или) затраты рассчитываются и (или) представляются в виде диапазона значений (максимальное, минимальное).

В таблице 2 указаны категории экономической ценности материальных и нематериальных активов, которые можно использовать при расчете инвестиций в информационную безопасность.

Таблица 2 — Типы экономической ценности организации

Тип ценности	Описание
Физическая	Сумма материальных активов организации
Ценность для клиентов	Оценка бизнеса, в основе которой лежит клиентская база организации

Окончание таблицы 2

Тип ценности	Описание
Общественная	Оценка общего восприятия обществом данной организации
Репутационная	Оценка восприятия организации ее конкурентами, поставщиками, клиентами, акционерами, государственными органами и прочими заинтересованными сторонами
Нематериальная и логически обосновываемая	Сумма нематериальных активов организации. В разряд нематериальных активов может также входить информация, находящаяся в распоряжении компании: стратегическая, коммерческая и т. п.

Модель базисных показателей ценности должна использоваться совместно с балансовой ведомостью для оценки и формирования заключений по экономическим аспектам ИБ. Такая модель имеет следующие характеристики.

Прямые показатели ценности выражаются в экономических категориях, таких как материальные потери или прямые инвестиции в зависимости от их реализации в пассивной или активной форме. В этой области возможны точные количественные значения.

Косвенные показатели ценности представляют собой расширенный вариант прямых показателей и отражают дополнительный рост или уменьшение ценности за счет учета нематериальных активов. Косвенные показатели ценности менее точны и сами по себе могут обозначаться диапазоном значений. Эти показатели могут отражать снижение объема выпуска продукции, увеличение административных издержек и т. п.

Расширенные показатели ценности зависят от прямых и косвенных показателей и могут быть весьма существенными. Расширенные показатели варьируются в более широком диапазоне, и их оценка может осуществляться аналогично оценке прямой и косвенной ценности. Однако в составе расширенных показателей могут рассматриваться многие другие факторы, например такие, как возможность отрицательного воздействия на общество и (или) на организацию в целом. Среди подобных факторов может, например, учитываться вероятность снижения стоимости акций предприятия (в зависимости от ситуации) и т. п. В этом смысле среди расширенных показателей могут учитываться факторы, которые невозможно выразить в количественной форме, например ценность бренда, потеря репутации и т. п. (следует отметить, что эти показатели чаще всего имеют отрицательные значения, хотя возможны и положительные).

Оценку своих информационных активов организация должна завершить анализом заинтересованных сторон, например:

a) материальных активов, формирующих организацию;

b) ценности бизнеса, формируемой клиентской базой;

c) нематериальных активов (информации, восприятия клиентами и обществом, ценности бренда и т. д.).

Таблица 3 — Типы стоимости экономической ценности (стоимости) активов. Принципы и примеры

Категория	Тип ценности	Описание	Актив	Ценность
A	Организация	Стороны в сфере действия СМИБ	Активы, обеспечивающие долгосрочную работу и поддержку бизнеса	Итоговое значение может отражать бизнес-процессы, связанные с конкретными активами, такими как права интеллектуальной собственности, базы данных, ресурсы ИКТ и прочее, которые могут выражаться в конкретных показателях
B	2-е и 3-и стороны	Отдельные клиенты, поставщики	Активы, обеспечивающие работу и поддержку бизнеса в отношении определенной стороны	Показатель для задействованных активов

Окончание таблицы 3

Категория	Тип ценности	Описание	Актив	Ценность
C	Заинтересованные стороны	Любая сторона, заинтересованная в аспектах ИБ организации, например ее владельцы	Активы, обеспечивающие работу и поддержку бизнеса в отношении определенной стороны	Итоговое значение может отражать бизнес-процессы, связанные с конкретными активами, такими как права интеллектуальной собственности, базы данных, ресурсы ИКТ и прочее, которые могут выражаться в конкретных показателях
D	Общественная	Интересы сообществ	Активы, которые могут отражать интересы сообществ	Показатель воздействия на сообщества и его опосредованного воздействия на организацию

Для этого метода определения ценности можно использовать градацию по определенным категориям. Например, информационные активы, связанные с базой данных, которая содержит персональные данные 100 000 клиентов, могут иметь намного большую ценность, если рассматривать интересы организации (категория A), других заинтересованных сторон (категория C) и прочих затрагиваемых сторон (категория B) в совокупности.

Градацию оценки также можно производить исходя из категорий важных активов. Например, база данных, в которой содержатся персональные данные 100 000 клиентов, может иметь большое значение для определенного правительственного учреждения. Аналогичным образом, неопубликованный пока окончательный финансовый отчет крупнейшей международной компании является сугубо конфиденциальным и сопряжен с риском инсайдерской торговли ценными бумагами и значительными последствиями для мировой экономики.

Организации могут принимать информированные экономические решения, увязывая между собой решения по расходам с соответствующими последствиями. Поскольку каждое решение по расходам (например, по расходам на уменьшение рисков, сертификацию) может иметь разнообразные последствия, соответствующую зависимость можно представить в виде таблицы.

8 Баланс экономических аспектов СМИБ

8.1 Введение

Для эффективной работы организации необходима система ИБ, которая обеспечивает защиту ее информационных активов от неблагоприятного воздействия и при этом сохраняет их доступность для тех пользователей, которым они необходимы для последовательного решения коммерческих задач такой организации. Как правило, общие требования, связанные с определением выгод и затрат при решении коммерческих задач организации, имеют отношение к следующему:

a) снижение материальных потерь (во многих случаях в годовом исчислении);

b) сведение к минимуму затрат, связанных с выделением финансового и прочего обеспечения на случай возникновения потерь (инцидентов);

c) эффективность программы менеджмента ИБ, направленной на защиту информационных активов;

d) эффективность программы ИБ, связанной с затратами на планирование, проектирование, реализацию, обслуживание и улучшение такой программы.

Менеджмент ИБ способен обеспечивать нематериальные (нефинансовые) и материальные (финансовые) преимущества, выражаемые в положительных значениях, когда руководство сохраняет возможность контролировать риски ИБ.

Решения о расходах должны быть увязаны с ожидаемыми преимуществами от снижения рисков благодаря развертыванию запланированных средств управления. Как правило, снижение рисков обеспечивается набором средств управления. Определенное средство управления может способствовать снижению рисков на различных уровнях, причем воздействие такого средства варьируется от незначительного уменьшения риска до полной его нейтрализации.

ИБ должна способствовать достижению коммерческих целей. Необходимо помнить, что для достижения коммерческих целей применяют различные подходы в зависимости от масштабов затрат и

получаемых преимуществ. Например, можно попытаться найти баланс между преимуществами быстрого вывода продуктов на рынок (и более быстрого получения дохода) и повышением риска возможных потерь вследствие инцидентов ИБ (например, недостаточной защиты конфиденциальности данных клиентов и, как следствие, доступа к ним посторонних лиц). В этом случае потенциальные убытки оцениваются на случай выбытия или повреждения информационного актива (данных клиентов). Как вариант, оптимальным решением может быть внедрение более дорогостоящей программы менеджмента ИБ, чтобы обеспечить преимущество в результате благоприятной реакции потребителей на продукты или услуги организации.

8.2 Экономические преимущества

Снижение убытков можно установить путем сравнения сумм ожидаемых годовых убытков при отсутствии или наличии определенной программы менеджмента ИБ. При проведении такого сравнения следует использовать методику, не входящую в противоречие с другими методиками, используемыми организацией.

В тех случаях, когда для определения риска ИБ используются иные критерии или методы оценки, экономические результаты в целом, скорее всего, не будут соответствовать результатам других программ и инициатив. Аналогичным образом, для обеспечения устойчивых и сравнимых результатов используемые для определения экономических преимуществ критерии рисков следует ограничить теми, которые преимущественно относятся к финансовой составляющей. Организация также должна изучить, как можно использовать неэкономические факторы после того, как будет завершена работа с финансово-экономическими показателями. Информация об управлении рисками ИБ приводится в ИСО/МЭК 27005.

Важно отметить, что отбор критериев рисков, связанных с определением финансово-экономических преимуществ, редко связан с функцией менеджмента ИБ и осуществляется в основном финансовым директором или другим сотрудником, выполняющим аналогичные функции.

Реализация программы менеджмента ИБ позволяет снизить расходы на предотвращение финансовых потерь и объем резервов на случай убытков. Это экономическое преимущество можно учесть при рассмотрении программы менеджмента ИБ.

8.3 Оптимальные затраты

Затраты на программу менеджмента ИБ для решения определенных коммерческих задач должны быть достаточными для реализации всего жизненного цикла программы с применением основанного на учете рисков подхода. Жизненный цикл программы обычно состоит из следующих этапов:

a) планирование;
b) реализация;
c) эксплуатация;
d) поддержка;
e) улучшение;
f) закрытие.

В сумме затрат необходимо также учесть процедуры отчетности и обеспечения эффективности (в том числе аудит со стороны клиентов, внутренний аудит с привлечением третьих сторон или иные процедуры обеспечения эффективности). Кроме этого, следует принять во внимание затраты на обучение и повышение осведомленности тех, кто применяет средства управления информационной безопасностью.

В затратах необходимо также учесть весь комплекс мер программы менеджмента ИБ (см. ИСО/МЭК 27001) и оценить их с учетом ожидаемых преимуществ, причем не только материальных (см. ИСО/МЭК 27004). Такой подход оправдан, поскольку зачастую бывает невозможно отнести к отдельным категориям затраты, связанные с материальными и нематериальными преимуществами.

Наличие данных о затратах и эффективности программы менеджмента ИБ обеспечивает дополнительное преимущество и повышает степень доверия к ней заинтересованных сторон.

В таблице 4 отражены основные области затрат, которые необходимо учитывать при оценке программы менеджмента ИБ.

Таблица 4 — Основные области затрат

Область затрат	Описание
Оценка рисков	Все затраты, связанные с выявлением рисков, их анализом и оценкой
Обучение, повышение уровня осведомленности	Все затраты на вводное обучение, программы в рамках всей организации, целевое обучение, оценку качества обучения, проверки, разработку обучающих материалов, докладчиков и средства мониторинга
Средства управления	Все прямые затраты на отбор и реализацию средств управления для снижения рисков, оперативные средства управления, прочие возможности обработки рисков, а также непрямые затраты, связанные с организационной эффективностью воздействий средств управления. Средства управления могут быть превентивными, детективными и (или) реагирующими
Сертификация	Все затраты, связанные с мониторингом и тестированием средств управления, функций обеспечения эффективности, сертификацией и всем, что необходимо для проверки эффективности средств управления безопасностью. Затраты на сертификацию оцениваются по расходам на персонал, выполняющий тестирование средств управления, расходам на аудит, обновление сертификатов или регистрацию в надзорных органах
Аудит	Затраты на услуги аудита [внутреннего и (или) внешнего]. Здесь должно быть учтено рабочее время внутреннего персонала, затрачиваемое на проведение аудита, а также на планирование, поддержку и контрольные процедуры
Измерения	Затраты на внешние и (или) внутренние ресурсы для реализации программ измерений, инструменты и их использование. Здесь необходимо также отразить рабочее время внутреннего персонала, затрачиваемое на получение результатов измерений

8.4 Экономические расчеты в отношении СМИБ

8.4.1 Обзор

Для решения задач ИБ необходимо технико-экономическое обоснование, в котором будут отражены экономические аспекты ИБ на основе модели расчета, представленной в приложении С.

В коммерческом обосновании инвестиций в ИБ необходимо учесть затраты, выручку и отдачу. Иными словами, необходимо обоснование для соответствующих вложений средств.

Поскольку каждый отдельный случай уникален, необходимо вырабатывать отдельный подход. Экономические аспекты ИБ не сильно отличаются от экономических моделей, используемых для обоснования инвестиций в маркетинг для повышения продаж. Преимущества в виде выручки и отдачи очень редко бывают самоочевидны, поэтому требуется проведение их оценки.

Экономические модели можно разделить на две категории, приведенные в 6.2. На рисунке 2 показана иерархия применения моделей. Отдельный метод можно применять на нескольких уровнях и по возможности обобщать. Обобщение легче использовать в экономических моделях категории В ввиду ограничения их области действия.

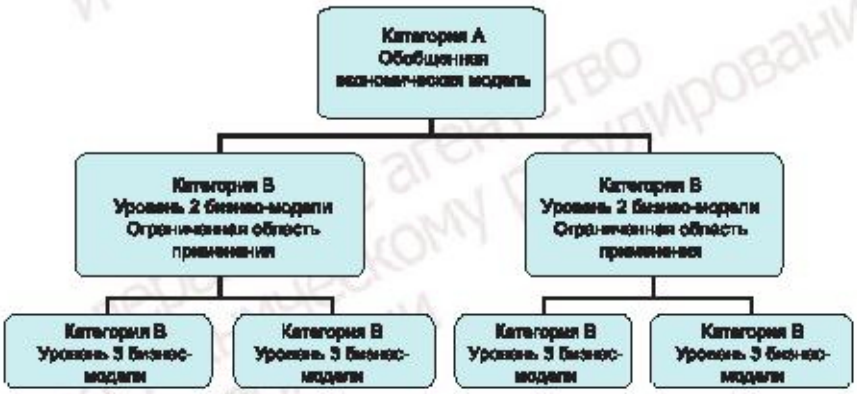

Рисунок 2 — Подход к формированию экономической модели менеджмента ИБ по принципу «снизу вверх»

Наиболее существенным различием при использовании экономической модели является следующее: общеорганизационная категория (A) часто работает по принципу «сверху вниз», тогда как категория (B) с более узкой областью применения — по принципу «снизу вверх».

При наличии точных данных общеорганизационную категорию (A) можно дополнить более детализированными моделями. В случае использования общеорганизационной модели (A) и частичной модели (B) на точность расчетов влияет следующее:

a) наличие информации, относящейся к экономическим расчетам, например стоимости активов, статистике и т. п.;

b) наличие ресурсов (времени, сотрудников, денежных средств и т. п.) для получения результатов;

c) наличие необходимых компетенций, например внутренних и внешних экспертов.

В рамках упрощенного подхода в качестве отправной точки можно использовать разделение на категории, после чего провести экономические расчеты на базе первичных расчетных данных.

8.4.2 Рекомендации

В рамках СМИБ необходимо выполнить следующие шаги, чтобы оценить коммерческую целесообразность использования экономической модели ИБ.

a) установление контекста:
   1) получение описания с коммерческой точки зрения (при наличии);
   2) определение сферы действия модели;
   3) определение среды реализации модели;
   4) определение заинтересованных сторон;
   5) определение круга лиц, принимающих коммерческие решения в рамках модели;
   6) определение категории модели;

b) определение активов, зависящих от ИБ в рамках модели, например:
   1) критически важная информация;
   2) система ИКТ;
   3) любые другие активы;
   4) ценность активов с точки зрения ИБ;
   5) базовый подход, используемый для расчетов, включая модели и обобщение;

c) определение задач модели:
   1) описание в качественном измерении;
   2) описание в количественном измерении;
   3) заключение в денежном выражении;

d) определение сроков:
   1) как долго планируется применять модель в организации:
      i) долгосрочные модели — более одного года (сколько именно);
      ii) краткосрочные модели — не более одного года;

e) определение затрат на реализацию модели, например:
   1) затраты в краткосрочной перспективе (в пределах одного года; не оказывают воздействия на организацию по истечении этого срока);
   2) инвестиционные затраты (единовременные затраты, которые в дальнейшем осуществлять не потребуется);
   3) текущие затраты — годовые затраты на реализацию модели;
   4) затраты уместнее рассматривать как прямые, косвенные или расширенные (см. также приложение C, модель C.3);

f) определение преимуществ и ценности модели, например:
   1) возможность обеспечить соответствие требованиям во избежание штрафов;
   2) возможность обеспечить соответствие требованиям и (или) повысить продажи благодаря выходу на новые рынки;
   3) возможность улучшить имидж и (или) повысить продажи благодаря выходу на новые рынки;
   4) положительное воздействие уменьшения рисков;
   5) повышение внутренней эффективности;
   6) ценность каждого информационного актива в случае нарушения его ИБ;
   7) любая другая сравнимая модель;
   8) возможность использования отрицательной стоимости в качестве полезной возможности (см. также приложение C);

g) использование возможных взаимозависимостей между стоимостью и ценностью.

Для всего перечисленного выше можно найти возможности применения, но зачастую среда реализации модели ограничивает использование элементов ценности. Информация о ценности может поступать из разных, но взаимосвязанных источников. Например, в ценность снижения рисков можно заложить отсутствие штрафов за несоответствие требованиям. Ценность ИБ зачастую отражает последствия, связанные с риском. В практических условиях можно использовать множество источников.

Подведение итогов для метода отбора:

1) в масштабах всей организации можно использовать модель базовой стоимости (BVM) и (или) общий инвестиционный расчет. Достаточно часто применяется комбинация обоих методов (см. модель категории А);

2) более узкая область применения в отношении актива и (или) средства управления дает основания использовать расчет коэффициента окупаемости инвестиций (см. модель категории В);

3) если среда и область реализации являются смешанными, можно применять оба метода с учетом специфики активов и их воздействия на конфиденциальность, целостность и доступность (см. модель категории В).

8.4.3 Экономическая модель на базе общеорганизационного подхода (категория А)

Можно применять модель с более широкой областью применения (категория А) с разбивкой экономических показателей и последующим их обобщением (снизу вверх) либо идентификацией посредством метода общего анализа (сверху вниз), при котором осуществляется оценка детализированных показателей. При использовании второго метода возможна значительная неопределенность, что может сделать его непригодным. При этом метод может казаться руководству достаточно точным для принятия решений. На его применение может быть потрачено много времени, а количественные результаты не оправдают затраченных усилий.

Этот метод можно реализовывать поэтапно. Метод в целом представляет собой процесс последовательных приближений, при котором входные данные меняются по мере получения информации вплоть до окончательного расчета. Зачастую бывает проще определить диапазон вводных значений или результатов, чем конкретное значение. Если возникает возможность применения диапазона значений, желательно отразить в документации минимальное и максимальное значения.

Положительное вводное значение:

a) прямые показатели возможного годового дохода, например за счет снижения издержек, связанных с инцидентом;

b) косвенные показатели возможного дохода, применяемые к модели во времени, например отсутствие штрафов за невыполнение требований;

c) расширенные показатели возможного дохода, применяемые к модели во времени, например повышение продаж благодаря выходу на новые рынки.

Отрицательное вводное значение:

d) прямые годовые затраты, например текущие затраты;

e) косвенная стоимость, применяемая к модели во времени, например запуск проекта;

f) расширенная стоимость, применяемая к модели во времени, например убытки от реализации.

Пример приводится в модели D.1 приложения D (с использованием модели, указанной в приложении С, С.2—С.5).

Расчет также может производиться в отношении задействованных активов (снизу вверх) с использованием принципа, изложенного в таблице 2. Этот подход дает более точные результаты, но требует больше усилий: его успешность зависит от определения активов, что во многих случаях является непростой задачей. Этот метод отражает подход «снизу вверх» и показан на рисунке 2.

8.4.4 Экономическая модель, применяемая к части организации (категория В)

Модель с частичным применением (категория В) означает, что все экономические показатели собираются на уровне деталей, после чего обобщаются (снизу вверх).

Сложность моделей категории частичного применения (категория В) может варьироваться очень значительно. На примерах моделей, приведенных в D.2 и D.3 приложения D, показано применение в более узкой и более широкой области.

Этот метод может быть реализован поэтапно. В целом, это процесс последовательного приближения, когда входные данные меняются по мере получения информации. Окончательный расчет возможен только после того, как будут внесены все изменения. Зачастую бывает проще определить диапазон вводных значений или результатов, чем конкретное значение. Если возникает возможность применения диапазона значений, желательно отразить в документации минимальное и максимальное значения.

Положительное вводное значение:

a) показатель конфиденциальности, целостности и доступности в пределах сферы действия модели;

b) прямое влияние на ценность с учетом риска, связанного с нарушением конфиденциальности, целостности и доступности;

c) превращение отрицательного воздействия в ценность возможности с обеспечением должного уровня ИБ для каждого сценария в отношении конфиденциальности, целостности и доступности (т. е. ни один из выявленных рисков не материализуется).

Отрицательное вводное значение:

d) прямые годовые затраты, например текущие затраты на снижение риска;

e) любая косвенная стоимость, применяемая к экономической модели во времени, например запуск проекта;

f) расширенная стоимость, применяемая к модели во времени, например убытки от реализации.

См. в качестве примера D.2 приложения D.

Экономическая модель с частичным применением (категория B) и очень ограниченной областью действия означает необходимость сбора всех экономических показателей на детальном уровне с последующим прямым их использованием в отношении модели.

Краткий анализ с отбором простого метода, например понятного для понимания и реализации модели с переходом от отрицательных значений к положительным (см. приложение C, C.5).

Положительное вводное значение:

a) оценка фактического или потенциального воздействия на коммерческую деятельность в связи с информационной безопасностью;

b) оценка положительного показателя ценности для деятельности в рамках экономической модели;

c) заключение о наличии каких-либо положительных значений в зависимости от типа деятельности и включении их в анализ (исключении из анализа). Заключение будет зависеть от конкретной модели и доступной информации.

Отрицательное вводное значение:

d) определение прямого(ых) и косвенного(ых) средства(средств) управления, необходимого(ых) для снижения воздействия;

e) определение прямых и косвенных затрат на применение средства(средств) управления.

Заключение:

f) определение чистой ценности и (или) стоимости;

g) сравнение и принятие решения.

См. приложение D, D.3.

Приложение А
(справочное)

Определение заинтересованных сторон и задач для установки значений

А.1 Обзор

Цель настоящего приложения — помочь организациям в оценке расширенного экономического воздействия внедрения программ менеджмента ИБ и связанных с ними инвестиций. Повышение качества менеджмента ИБ в организации может положительно сказаться на множестве элементов ее деятельности.

Характер и объем положительного экономического воздействия будет зависеть от того, насколько организации удастся использовать преимущества, связанные с эффективным менеджментом ИБ.

А.2 Государственные и частные сектора экономики, где безопасность имеет критическое значение

Государственные и частные организации тех секторов экономики, в которых информационная безопасность является основной задачей (например, банковское дело, правительственные структуры, здравоохранение и оборонная отрасль), очевидным образом зависят от внедряемых и используемых мер ИБ. Это определяет ценность их бренда и имидж, а также ценность их продуктов и услуг. По тем же причинам инциденты ИБ в организациях вышеупомянутых секторов могут наносить вред их репутации и, в худшем случае, приводить к прекращению их деятельности.

А.3 Здравоохранение и общественная безопасность

Настоящий стандарт не имеет прямого воздействия на предприятия общественного здравоохранения и безопасности. Однако он косвенно воздействует на аспекты безопасности разнообразных форм медицинской помощи. С его помощью можно убедиться в их надлежащей защите.

А.4 Общественность и сообщества

Настоящий стандарт может широко применяться в организациях, работающих в самых разных отраслях общественной деятельности или связанных с ними. Его негативное воздействие на меньшинства или слабо защищенные слои населения маловероятно по сравнению с ощутимыми преимуществами для всех заинтересованных сторон, а также общества и сообществ в целом.

А.5 Персональная информация

В тех случаях, когда информация затрагивает интересы частных лиц и их права на личную жизнь, настоящий стандарт может иметь положительное воздействие: стандарт может обеспечить повышение уровня защиты персональной и конфиденциальной информации в организациях, использующих его наряду со СМИБ.

Для большинства организаций управление большими хранилищами персональной информации сопряжено с повышенными рисками ИБ. Нарушение безопасности персональных данных может приводить к отрицательным внешним последствиям деятельности.

А.6 Охрана окружающей среды

Настоящий стандарт не предполагает какого-либо значительного прямого воздействия на охрану окружающей среды.

Настоящий стандарт может иметь косвенное положительное воздействие на охрану окружающей среды в связи с тем, что информация, имеющая большое значение для управления вопросами охраны окружающей среды, будет лучше защищена в тех организациях, которые используют этот стандарт вместе с существующей системой менеджмента ИБ.

А.7 Конкуренция

Организации, обеспечивающие надлежащий уровень ИБ, могут обеспечить себе конкурентное преимущество благодаря лучшему управлению соответствующими рисками.

Приложение В
(справочное)

Экономические решения и основные факторы принятия решений в отношении затрат

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
A	Возможность для предприятий участвовать в проектах с повышенными рисками благодаря развитой системе управления рисками и снижению собственных рисков по сравнению с конкурентами	Да. Системы, обеспечивающие снижение рисков, открывают возможности для деятельности в среде с повышенными рисками	Да. Возможность продемонстрировать наличие сертификатов безопасности может способствовать вовлечению в мероприятия по безопасности партнеров по бизнесу	Да. Партнеры по бизнесу с большей вероятностью примут участие в более рискованных проектах, если организация способна продемонстрировать более зрелую систему управления рисками	Да. Как правило, применяется расширенный спектр средств управления, воздействующий на всю коммерческую деятельность (например, программа обучения). Стоимость каждого отдельного средства управления зависит от его типа, а также от зрелости системы ИБ организации
B	Возможность для предприятия обеспечить соответствие нормативным требованиям и избежать ограничений деятельности и штрафов	Да. Отношения организации с регулирующими органами напрямую зависят от качества ее системы снижения рисков	Возможно. Сертификация может напрямую способствовать выполнению нормативных требований	Нет. Увеличение расходов организации на систему управления рисками не влияет напрямую на ее отношения с регулирующими органами	Да. Как правило, применяется расширенный спектр средств управления, воздействующий на всю коммерческую деятельность, а также на отдельные технические средства управления. Стоимость каждого отдельного средства управления зависит от его типа, а также от зрелости системы ИБ организации
C	Повышение разноплановости, маневренности предприятия и скорости его реагирования на изменения, например благодаря повышению гибкости решений в области безопасности	Нет. Снижение рисков не всегда повышает маневренность предприятия	Нет. Сертификация не повышает маневренность предприятия	Да. Увеличение расходов на управление операционными рисками может способствовать повышению способности предприятия использовать возможности с повышенным риском	Нет. Как правило, средства управления не способствуют повышению маневренности предприятия. Влияние в большей степени относится к СМИБ и степени ее зрелости

Продолжение таблицы

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
D	Выход на приемлемый уровень прогнозируемых (будущих) убытков исходя из ожидаемого профиля риска, например благодаря снижению рисков (ожидаемые потери в годовом исчислении)	Да. Снижение рисков напрямую определяет уровни ожидаемых убытков	Нет. Сертификация не влияет непосредственно на снижение рисков и ожидаемые уровни убытков	Да. Повышение расходов на управление операционными рисками в большей степени способно снизить риски и ожидаемые убытки	Да. Средства управления могут непосредственно влиять на снижение рисков
E	Ожидаемые потери в годовом исчислении (ALE) отражают результат ожидаемых значений (средних значений) убытков, а также их появления. Такие расчеты уровня риска не обеспечивают достаточных результатов для редко случающихся инцидентов и (или) инцидентов с большой степенью воздействия. Средства ИБ также должны учитывать подобные редко встречающиеся инциденты и (или) инциденты с большой степенью воздействия ввиду их существенного значения для ИБ. Расчет стоимости под риском. Показатель стоимости под риском может обеспечивать более приемлемые результаты по сравнению с ALE	Да. Снижение рисков напрямую определяет уровни ожидаемых убытков	Нет. Сертификация не влияет непосредственно на снижение рисков и ожидаемые уровни убытков	Да. Повышение расходов на управление операционными рисками в большей степени способно снизить риски и ожидаемые убытки	Да. Средства управления могут непосредственно влиять на снижение рисков
F	Ожидаемые потери в годовом исчислении (ALE) отражают результат ожидаемых значений (средних значений) убытков, а также их появления. Такие расчеты уровня риска не обеспечива-	Да. Снижение рисков напрямую определяет уровни ожидаемых убытков	Нет. Сертификация не влияет непосредственно на снижение рисков и ожидаемые уровни убытков	Да. Повышение расходов на управление операционными рисками в большей степени способно снизить риски и ожидаемые убытки	Да. Средства управления могут непосредственно влиять на снижение рисков

Продолжение таблицы

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
F	ют достаточных результатов для очень редко случающихся инцидентов и (или) инцидентов с очень большой степенью воздействия. При этом средства ИБ также должны учитывать подобные очень редко случающиеся инциденты и (или) инциденты с очень большой степенью воздействия. Расчет средних ожидаемых убытков может обеспечивать более приемлемые результаты по сравнению с ALE				
G	Поддержание репутации и цены акций предприятия путем повышения элементов доверия, например прохождением сертификации для выполнения требований стандартов и снижения рисков с возможными серьезными последствиями для репутации предприятия	Да. Возможность снижения репутационных рисков	Да. Прохождение сертификации может способствовать улучшению репутации	Да. Повышение расходов на управление операционными рисками может способствовать улучшению репутации, особенно для будущих сотрудников	Нет. Средства управления не оказывают прямого влияния на цену акций. Влияние в большей степени относится к СМИБ и степени ее зрелости
H	Сведение к минимуму ожидаемых операционных затрат на работу системы ИБ и управления рисками, например благодаря повышению эффективности	Нет. Снижение рисков может не привести к повышению эффективности операций	Нет. Сертификация может не привести к снижению операционных издержек	Нет. Увеличение расходов на управление рисками может не привести к прямому повышению эффективности	Нет. Средства управления напрямую не способствуют повышению эффективности, связанному с управлением рисками. Влияние в большей степени относится к СМИБ и степени ее зрелости, в том числе к повышению уровня осведомленности, измерениям, аудитам и т. п.

Продолжение таблицы

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
I	Обеспечение полноты и точности отчетности по управлению информационными рисками	Да. Увеличение вложений в меры обеспечения способно помочь в выявлении неэффективной обработки рисков и способствовать дальнейшим улучшениям	Да. Сертификация обеспечивает некоторое повышение надежности процессов	Да. Увеличение численности персонала повышает функциональность мер по обеспечению	Нет. Средства управления не влияют напрямую на управление рисками. Влияние в большей степени относится к СМИБ и степени ее зрелости, в том числе к повышению уровня осведомленности, измерениям, аудитам и т. п.
J	Защита персонала от личной ответственности, например путем проведения комплексной юридической оценки для устранения возможной ответственности директоров	Да. Недостаточные вложения в снижение рисков могут приводить к неосмотрительным действиям директоров	Да. Получение сертификатов внешних организаций может дать директорам возможность продемонстрировать результаты правового аудита	Да. Недостаточные вложения в управление рисками могут приводить к неосмотрительным действиям директоров	Да. Средства управления ролями и ответственностью за обеспечение ИБ
K	Соответствие ожиданиям сообществ в качестве поставщика инфраструктуры и услуг путем защиты их информации	Да. Возможность снижения рисков для информации клиентов	Да. Для повышения уровня защиты информации клиентов может использоваться сертификация	Нет. Повышение расходов на управление рисками не приводит напрямую к улучшению защиты информации клиентов	Нет. Средства управления напрямую не влияют на повышение уровня ожиданий сообществ. Влияние в большей степени относится к СМИБ и степени ее зрелости, в том числе к повышению уровня осведомленности, измерениям, аудитам и прочего для предоставления обратной связи сообществу
L	Предоставление возможностей трудоустройства членам сообществ	Да. Вложения в снижение рисков обеспечивают возможности для трудоустройства занятых в этой сфере	Нет. Сертификация не влияет напрямую на возможности для трудоустройства	Да. Повышение вложений в управление рисками создает дополнительные возможности для трудоустройства	Нет. Средства управления напрямую не влияют на расширение возможностей для трудоустройства членов сообществ. Влияние в большей степени относится к СМИБ и степени ее зрелости, в том числе к повышению уровня осведомленности, измерениям, аудитам и т. п.

Продолжение таблицы

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
M	Отсутствие требований в отношении расходов на снижение риска и аудиты, а также дополнительные меры контроля, благодаря обеспечению приемлемых параметров работы	Да. Снижение рисков является средством, позволяющим избежать необходимости выделения средств на нейтрализацию рисков и проведение аудитов	Нет. Маловероятно, что сертификация напрямую повлияет на уменьшение потребности в выделении средств на нейтрализацию рисков и проведение аудитов	Нет. Увеличение расходов на управление рисками не приводит непосредственно к снижению требований в отношении выделения средств на нейтрализацию рисков и проведение аудитов	Нет. Средства управления не влияют напрямую на необходимость в выделении средств на нейтрализацию рисков и проведение аудитов (за исключением случаев, когда такие средства управления отсутствуют)
N	Отсутствие воздействий на внешние стороны, такие как поставщики инфраструктуры и услуг	Да. Общее снижение рисков может привести к уменьшению рисков воздействия на внешние стороны, поставщиков инфраструктуры и услуг	Нет. Сертификация не приводит к непосредственному уменьшению воздействия на внешние стороны	Нет. Увеличение расходов на управление рисками не приводит непосредственно к уменьшению риска для внешних сторон	Да. Средства контроля могут напрямую содействовать предотвращению воздействий
O	Системы для управления политиками, процедурами безопасности и прочим, а также их распространения	Да. Возможность снижения риска ошибок из-за человеческого фактора	Да. Является предметом аудита для прохождения сертификации и оказывает соответствующее влияние	Нет. К повышению затрат на организацию управления рисками не приводит	Нет. Средства управления напрямую не влияют на обучение. Влияние в большей степени относится к СМИБ и степени ее зрелости, в том числе к повышению уровня осведомленности, измерениям, аудитам и т. п.
P	Системы идентификации и (или) аутентификации и управления доступом для контроля идентификаторов пользователей, прав доступа и (или) разрешений и т. п. для систем приложений	Да. Возможность снижения риска утраты конфиденциальности и целостности информации, а также повышения затрат на обработку информации и соответствующие технические решения	Нет. Может быть предметом аудита при прохождении сертификации	Нет. К повышению затрат на организацию управления рисками не приводит	Да. Применяются соответствующие средства управления

Окончание таблицы

Дополнительные материалы	Коммерческие задачи	Решения в отношении затрат			
		Затраты на снижение рисков	Затраты на сертификацию	Организационные затраты на управление рисками	Затраты на средство управления
Q	Системы управления уязвимостями и изменениями для обновления мер защиты при помощи исправлений безопасности	Да. Возможность снижения рисков, связанных с утратой конфиденциальности и целостности. Возможность повышения расходов на обработку данных, а также технические решения	Нет. Может быть предметом аудита при прохождении сертификации	Нет. К повышению затрат на организацию управления рисками не приводит	Да. Применяются соответствующие средства управления
R	Инциденты с оценочной стоимостью, достаточной для обоснования создания СМИБ, способной обеспечить общую экономию. Оценка данных производится с применением осторожного, рационального подхода с целью преодоления кризиса управления; одного лишь снижения затрат, связанных с инцидентами, бывает достаточно для обоснования расходов на СМИБ, хотя ими экономическая модель не исчерпывается	Да. Учет инцидентов в процессах обработки рисков повышает уровень сложности, но также обеспечивает более точные результаты оценки	Нет. Может быть предметом аудита при прохождении сертификации	Да. Может привести к увеличению организационных затрат на управление рисками	Да. Применяются соответствующие средства управления
S	Работа с рисками ИБ и средствами управления в соответствии с требованиями рынка, законодательства или нормативного регулирования	Да. Должно быть основным элементом процесса обработки рисков	Да. Часть процесса сертификации	Да. Возможно повышение уровня управления рисками в организации	Да. Применяются средства управления соответствием требованиям

Приложение С
(справочное)

Экономические модели обеспечения информационной безопасности

С.1 Общая информация

Существует множество моделей расчетов, связанных с экономикой. Для целей ИБ можно использовать как эти, так и другие модели. В этом приложении приведены самые базовые модели.

Бывает сложно определить точные экономические последствия реализации процессов, процедур или технических средств для обеспечения ИБ. По этой причине результаты расчетов рекомендуется представлять в виде диапазонов значений (максимальных и минимальных). Этот момент не учитывается в моделях, поскольку используется одна модель, но с разными значениями и (или) показателями затрат.

С.2 Модель базовой стоимости

Основная модель базовой стоимости 1 применяется как к положительным (прибыль), а так и отрицательным (издержки) значениям. Ее следует использовать при работе с переходом от отрицательных значений к положительным и балансовой ведомостью. Данные выводятся в таблице с полным набором шагов по оценке и представлению результатов.

В основе принципа BVM 1 лежат следующие три области с различными характеристиками.

Прямые показатели ценности выражаются в экономических категориях, таких как материальные потери или прямые инвестиции в зависимости от их реализации в пассивной или активной форме. В этой области возможны точные количественные значения.

Косвенные показатели ценности представляют собой расширенный вариант прямых показателей и отражают дополнительный рост или уменьшение ценности за счет учета нематериальных активов. Косвенные показатели ценности менее точны и сами по себе могут обозначаться диапазоном значений. Эти показатели могут отражать снижение объема выпуска продукции, увеличение административных издержек и т. п.

Расширенные показатели ценности зависят от прямых и косвенных показателей и могут быть весьма существенными. Расширенные показатели варьируются в более широком диапазоне, и их оценка должна осуществляться аналогично оценке прямой и косвенной ценности. Однако на расширенные показатели могут влиять другие факторы, например такие, как возможность отрицательного влияния на общество и (или) на организацию в целом, например снижение стоимости акций и т. п. Такие расширенные показатели, как, например, ценность бренда или потеря репутации невозможно выразить в количественной форме. (Следует отметить, что эти показатели обычно имеют отрицательные значения, хотя возможны и положительные, как следствие внедрения ИБ.)

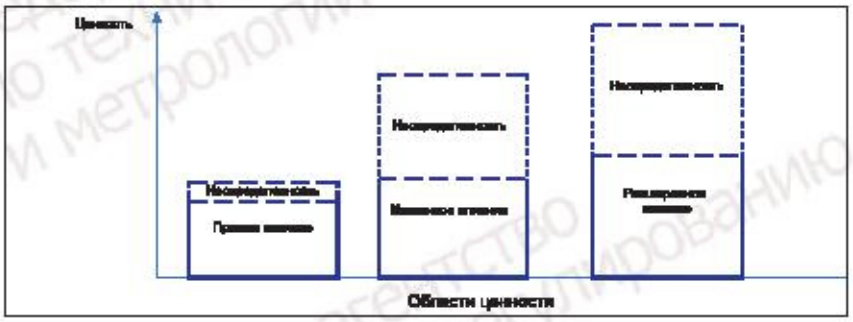

Рисунок С.1 — Основная модель базисных показателей ценности

С.3 Модель с переходом от отрицательных значений к положительным

Подход с переходом от отрицательных значений* к положительным* основан на взаимоисключающих вопросах:

- Насколько отрицательным будет значение, если мера не будет предпринята?
- Насколько положительным будет значение, если мера не будет предпринята?
- Насколько отрицательным будет значение, если мера будет предпринята?
- Насколько положительным будет значение, если мера будет предпринята?

Примечание — Значения, используемые в модели в качестве затрат, могут быть положительными.

Ответы на эти вопросы в сочетании с основной моделью базовой стоимости, показанной на рисунке С.1, формируют четыре квадрата, показанные на рисунке С.2.

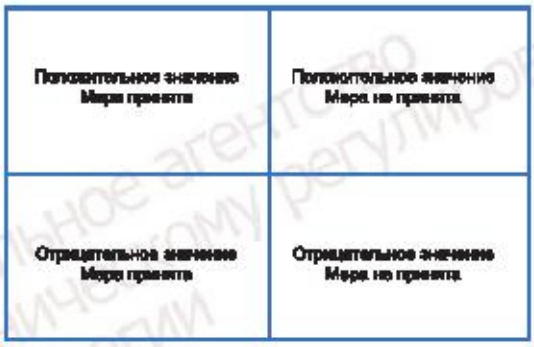

Рисунок С.2 — Модель перехода от отрицательных значений к положительным

Использование такой модели обеспечивает учет всех аспектов. Однако в отношении одной меры создаются дублирующие значения. Этого можно избежать, если использовать простую таблицу (см. рисунок С.1).

В таблице С.1 в некоторых случаях значение в ячейке A1 аналогично значению в ячейке D2, что делает возможным переход от отрицательного значения (стоимости) к положительному при сравнении чистого значения по результатам двух столбцов (1 и 2).

[Для более сложных мероприятий можно добавить новые строки, но при этом сравнение должно производиться между текущим состоянием (возможная мера не принята) и состоянием, при котором мера принята или реализована в полной мере].

Таблица С.1 — Таблица сравнения чистых значений

	Базовое положение	Мероприятие	Положительное значение — мера принята	Положительное значение — мера не принята	Отрицательное значение — мера принята	Отрицательное значение — мера не принята	Чистый результат
Дополнительные материалы			A	B	C	D	
1	Мера, способная изменить текущее положение дел	Мера «X» принята	*Ценность*	Неприменимо	*Стоимость*	Неприменимо	*1A—1B*
2	Возможная мера не принята	Мера «X» не принята	Неприменимо	*Ценность*	Неприменимо	*Стоимость*	*2B—2D*
Примечание — В настоящей таблице отражен основной принцип. Для дальнейшего упрощения можно удалить не соответствующие ситуации ячейки.							

С.4 Общий баланс инвестиций в меры защиты (теория сравнения затрат и ценности)

Теория заключается в том, что точку оптимального баланса можно найти путем постепенного применения к ценности затрат на защитные мероприятия. Оптимальная стоимость издержек по защите актива и ценности достигается в тех условиях, когда снижение риска, влияющее на стоимость, окажется меньше стоимости реализации меры по защите. В основе теории лежат следующие базовые факторы:

a) известная ценность (константа);

b) известные расходы на защиту (с возможностью роста в зависимости от принимаемых мер);

c) снижение риска в связи с применением мер защиты, что зависит от ценности и эффективности таких мер.

Ценность и расходы на меры защиты часто можно установить точно, но степень снижения является оценочной.

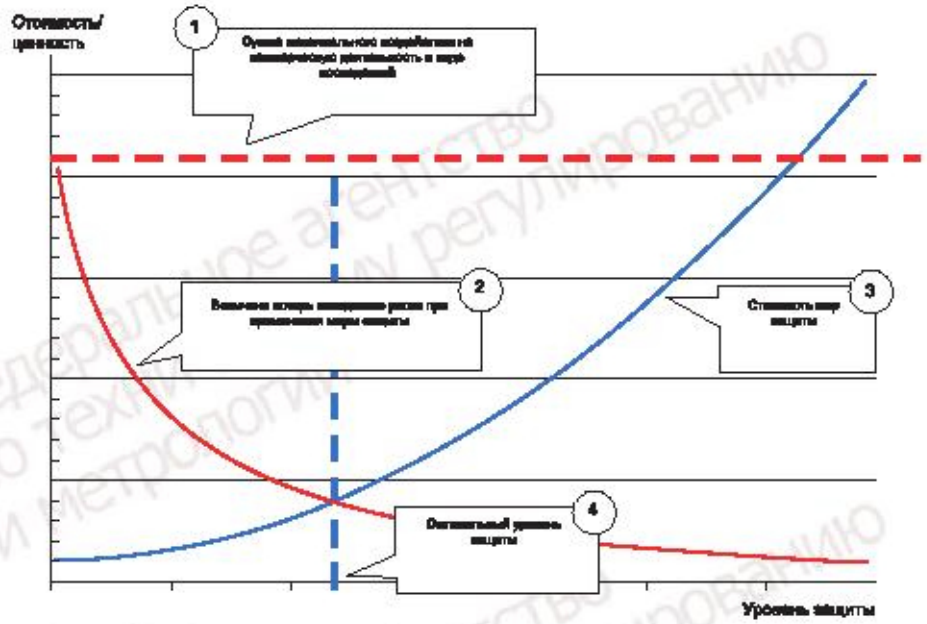

Рисунок С.3 — Теория оптимального баланса между стоимостью защитных мер и ценностью

С.5 Расчет общих инвестиций. Расчет затрат и ценности

Затраты. Анализ преимуществ часто используется государственными и прочими организациями, в том числе коммерческими, для оценки необходимости вмешательства. Анализ эффективности различных вариантов затрат призван установить, превышают ли преимущества объем вложений [т. е. имеет ли смысл что-либо делать в принципе и, если да, то насколько (какой вариант вмешательства выбрать)]. Цель состоит в оценке эффективности возможных мер по сравнению друг с другом и с текущей ситуацией. Для достижения наилучших результатов текущая ситуация меняется с применением эффективности по Парето.

Ниже приводится список шагов в рамках общего анализа затрат и преимуществ:

a) подготовка набора альтернативных проектов (программ);
b) составление списка основных участников (имеющих статус или влияние);
c) подбор системы измерения и сбора всех элементов затрат и выгод;
d) прогноз результата в виде затрат и выгод в течение срока реализации проекта;
e) перевод всех итоговых затрат и выгод в денежный эквивалент в местной валюте;
f) применение ставки дисконтирования (или внутреннего финансового курса)*;
g) расчет чистой текущей ценности вариантов реализации проекта;
h) анализ чувствительности;
i) рекомендации.

---

* *Чаще всего предоставляется финансовым отделом.*

Приложение D
(справочное)

Примеры расчета экономических моделей

D.1 Пример расчета экономической модели (вариант А)

Описание. Коммерческая организация сталкивается с растущим числом инцидентов ИБ, связанных с клиентами, в результате чего возникает необходимость в реализации требований стандарта ИСО/МЭК 27001. Отдел маркетинга направляет запрос о необходимости сертификации в соответствии с ИСО/МЭК 27001. Главный сотрудник по вопросам ИБ должен рассчитать экономическую модель реализации СМИБ в соответствии со стандартом ИСО/МЭК 27001 и включить в нее достаточно вводных данных, чтобы руководство запустило проект по реализации требований (см. ИСО/МЭК 27003).

Контекст. Сертификация производится в рамках всей организации.

В расчетах необходимо учесть, что технико-экономическое обоснование СМИБ будет оказывать долгосрочное воздействие на организацию. Расчет ценности и издержек может производиться на определенный предполагаемый период времени. В рамках упрощенного подхода решение о вложении средств принимается исходя из ситуации на момент принятия решения (например, 1 год), после чего производится сравнение с результатами за год без учета динамики. В качестве отправной точки для расчета экономической модели принимается второй вариант. Для учета фактора неопределенности используются минимальное и максимальное значения (диапазон значений). Далее по мере необходимости учитывается временное измерение.

Пункт	Факторы	Базовые (диапазон)	Относящиеся к ценности			Относящиеся к стоимости		
			Направление	Косвенное влияние	Расширенное влияние	Направление	Косвенное влияние	Расширенное влияние
A	Годовой оборот	100 млн $	x	100 млн $ · 3 % = = 3 млн $	x	x	x	x
B	Возможный рост продаж за год после сертификации	3 % (1 %—5 %)	x	x	x	x	x	x
C	Срок инвестиции	10 лет	x	x	x	x	x	x
D	Стоимость проекта реализации СМИБ	(± 20 %)	x	x	x	**0,5 млн $**	x	x
E	Стоимость сертификации в рамках проекта	н/д	x	x	x	**0,3 млн $**	x	x
F	Потеря внутренней эффективности при реализации проекта	(± 20 %)	x	x	x	x	Не оценивается*	x
G	Стоимость реализации средств управления СМИБ для сертификации в течение проекта	(± 20 %)	x	x	x	**0,3 млн $**	**0,2 млн $**	x
H	Годовая стоимость обслуживания СМИБ	x	x	x	x	**0,1 млн $**	x	x
I	Ежегодный прирост внутренней эффективности*	Не оценивается*	x	Не оценивается*	x	x	x	x
J	Экономия от проведения меньшего количества проверок*	Не оценивается*	Не оценивается*	Не оценивается*	x	x	x	x

Окончание таблицы

Пункт	Факторы	Базовые (диапазон)	Относящиеся к ценности			Относящиеся к стоимости		
			Направление	Косвенное влияние	Расширенное влияние	Направление	Косвенное влияние	Расширенное влияние
K	Экономия от снижения рисков*	Не оценивается*	Не оценивается*	Не оценивается*	Не оценивается*	x	x	x
L	Экономия от выполнения требований*	Не оценивается*	Не оценивается*	Не оценивается*	Не оценивается*	x	x	x
M	Ценность имиджа/бренда*	Не оценивается*	x	x	Не оценивается*	x	x	x
N	Общая стоимость сертификации в годовом исчислении (за исключением первоначальной стоимости)	Не оценивается*	x	x	x	Не оценивается*	x	x

* Эти (и прочие) затраты и (или) преимущества можно оценить в рамках экономической модели и включить в расчеты, если они могут оказать воздействие на практические аспекты принятия решения.

Примечание — Результаты вычислений приводятся исключительно в целях иллюстрации и не относятся к какой-либо реальной ситуации.

Первичные расчеты по заключению основаны на оценочных значениях без указания диапазона возможных значений.

Заключение 1 БАЗА:

В течение года после сертификации расширенный показатель имеет следующее значение:	3,0 млн $
Затраты обобщаются в следующем виде:	–1,4 млн $
Сумма:	+1,6 млн $

Заключение 2 Диапазон значений:

Второй расчет по заключению сделан на базе расчетных значений с использованием диапазона от максимальных значений (max) до минимальных (min). Максимальные значения представляют собой наибольшую ценность и наименьшие затраты, а минимальные значения — наименьшую ценность и максимальные затраты. (Изменения из-за неопределенности диапазонов отражены в таблице выше.)

Max:	В течение года после сертификации расширенный показатель max имеет следующее значение:	5,00 млн $
	Затраты по расчету 1 уменьшаются на 20 %: – 1,4 млн $ · 80 % =	–1,12 млн $
	Сумма:	+3,88 млн $
Min:	В течение года после сертификации расширенный минимальный показатель имеет следующее значение:	1,00 млн $
	Затраты по расчету 1 увеличиваются на 20 %: –1,4 млн $ · 120 % =	–2,35 млн $
	Сумма:	–1,35 млн $

Заключение 2 показывает, что, несмотря на более позитивный экономический сценарий по сравнению с другим возможным, вероятна ситуация, когда экономическая модель может оказаться убыточной. Это указывает на необходимость дополнительного анализа. Следует сделать перерасчет значений min, возможно, с большим количеством оценочных значений по факторам, указанным в таблице. Это позволит проверить, смогут ли дополнительные показатели ценности и затрат изменить отрицательный экономический результат расчета.

В качестве отправной точки должен использоваться вероятностный анализ, поскольку именно он способен дать четкие указания на незначительную вероятность, что может быть отражено в качестве причины использования расчета 1 как основы экономической модели.

Такой анализ для несертифицированной организации мог бы стать предложенной отделом продаж и маркетинга альтернативой, указывающей на возможное падение продаж на 15 % в течение трех лет. Это имеет отношение к той части клиентов организации, которые уже задают вопросы о выполнении требований ИСО/МЭК 27001.

[Падение на 15 % является очень большим (такое отрицательное значение оказывает положительное воздействие на мотивацию данной экономической модели), в сравнении с расчетами 1 и 2, а также показывает, что дополнительный анализ не приведет к существенным изменениям.]

Экономическую модель можно представить расчетом с альтернативным сценарием на базе вероятностного анализа.

D.2 Пример расчета частичной экономической модели (вариант Б)

Модель. Этот пример экономической модели относится к определенному активу, к которому могут применяться различные средства управления информационной безопасностью. В связи с этим данная модель имеет ограниченную область применения. В примере не учитываются затраты на средства управления, но учитываются издержки, связанные с неиспользованием средств управления, которые можно рассматривать как положительные значения для нейтрализации суммы расходов на средства управления на втором этапе. В рамках экономической модели принято решение о переходе на следующий этап для определения средств управления и связанных с ними затрат.

Информационный актив

База данных организации насчитывает 250 000 клиентов. Эта база содержит персональную информацию о каждом клиенте, сведения о личной кредитной карте и архив операций, осуществленных между клиентом и организацией за последние 10 лет.

Риски и сопутствующие издержки из-за возможных воздействий

Риски для информационного актива необходимо рассмотреть и оценить с точек зрения конфиденциальности, целостности и доступности (CIA).

Фактор CIA	Описание риска	Затраты организации
Конфиденциальность	База данных становится доступной для посторонних лиц и полностью копируется. Теперь эта информация используется для выяснения персональных данных клиентов организации и проведения несанкционированных операций с использованием этих персональных данных и сведений о кредитных картах клиентов	- Все клиенты должны быть оповещены о раскрытии их персональной информации посторонним лицам (25 $ по каждому клиенту). (Число клиентов, чья информация была украдена, насчитывает 1000 человек.) - В результате потери данных клиентов нарушено законодательство (единовременный штраф в размере 500 000 $). - Организация должна направить ресурсы на выяснение причины взлома, содействие правоохранительным органам в расследовании нарушения и очистку информационной системы во избежание нового взлома (единовременные расходы в размере 250 000 $)
Целостность	Клиент организации инициирует онлайн-операцию, и в ходе ее проведения раскрываются персональная информация и (или) детали другой организации	Каждую операцию необходимо проверить на наличие правильных данных (25 $ за одну операцию). (Количество операций, задействованных при взломе, составляет 10 000.) В результате несанкционированного отображения информации клиента нарушено законодательство (единовременный штраф в размере 500 000 $). Потеря клиентов, которые уходят к конкурентам (каждый клиент обходится в 100 $). [Взлому подверглись данные 40 % клиентов (1000)]
Доступность	База данных повреждена, и авторизованные пользователи не имеют доступа к информации	- Организации необходимо выделить ресурсы на определение причины потери данных и принятие мер для восстановления доступа [в том числе вызов консультантов (5000 $/час)]. (Расчетное количество часов: 300.) - Простой в работе персонала из-за невозможности осуществления операций (100 000 $ в час). (Расчетное количество часов: 10.) - Потеря текущего дохода из-за невозможности выполнения операций клиентами (100 $ по каждому клиенту, не имеющему возможности совершать операции). [Число клиентов, подвергшихся взлому, оценивается в 20 % (1000)]

В следующей таблице сумма затрат представляет собой общую ценность, уравновешивающую затраты на средства управления на следующем этапе:

CIA	В связи с клиентами	По законодательству	Перерыв в коммерческой деятельности	Необходимость выделения ресурсов	Сумма
Конфиденциальность	25 $ · 1000 = 25 000 $	500 000 $	x	250 000 $	775 000 $
Целостность	25 $ · 10 000 = 250 000 $ 100 $ · (40 % · 1000) = 40 000 $	500 000 $	x		790 000 $
Доступность	100 $ · (20 % · 1000) = 20 000 $	x	100 000 $ · 10 = = 1 000 000 $	5000 $ · 300 = = 1 500 000 $	2 520 000 $
Сумма	335 000 $	1 000 000 $	1 000 000 $	1 750 000 $	**4 085 000 $**

D.3 Пример актива/модели управления (пример Б)

Модель. Предоставление пользователям расширенной информации о правилах пользования Интернетом. Эта экономическая модель связана с конкретной мерой и имеет очень ограниченный набор средств управления. Даже в случае применения средств управления в масштабах всей организации такая экономическая модель считается ограниченной из-за незначительного количества средств управления. В рамках СМИБ принято решение о реализации этой меры.

Базовые данные:

Число пользователей:	1000
Ежегодные убытки от инцидентов, связанных с использованием Интернета:	100 000 $
Уменьшение числа инцидентов вследствие обучения:	70 %
Стоимость обучающих материалов:	10 000 $
Стоимость часа рабочего времени организации:	50 $
Количество часов обучения:	1
Срок, в течение которого результаты обучения остаются актуальными:	3 года
Срок расчета:	3 года
Количество сессий обучения:	2

На основе модели С.3 сделаны следующие расчеты и проведен анализ воздействия:

Мероприятие	Положительное значение	Отрицательное значение/затраты	Чистый результат
Проведение обучения интернет-пользователей	210 000 $ (3 · 100 000 · 70 %)	110 000 $ (10 000 + (50 · 1000 · 2)	+100 000 $
Без проведения обучения интернет-пользователей:	100 000 $ (50 · 1000 · 2)	300 000 $ (3 · 100 000)	–250 000 $

Заключение. Выраженная в чистом виде выгода от проведения обучения составляет 100 000 $ за три года. Убыток/издержки вследствие отсутствия обучения составляют –250 000 $.

Этот расчет может служить основой для принятия решения о реализации меры и последующего отслеживания его правильности. При наличии существенных расхождений необходимо определить дополнительные меры и произвести расчеты. (Пример может быть более сложным в связи с выявлением новых типов инцидентов. Считается, что все использованные в примере инциденты связаны с пользователями.)

В ходе анализа чувствительности расчета определяется, насколько необходимо уменьшить воздействие инцидента для достижения точки равновесия. Это делается с использованием таблицы в обратном порядке: положительное значение берется равным отрицательному (ценность/затраты), чтобы чистое значение было равно нулю. В следующей таблице показан повторный расчет положительного значения для получения порога безубыточности нейтрализации инцидента.

Мероприятие	Положительное значение	Отрицательное значение/затраты	Чистый результат
Проведение обучения интернет-пользователей	110 000 $ (3 · 100 000 · Y = 110 000 $) Y = 110 000/3 · 100 000 (%) = 37 %	110 000 $ (10 000 + (50 · 1000 · 2)	0 $

Анализ чувствительности показывает, что для достижения порога безубыточности обучения достаточно снижения количества инцидентов лишь наполовину. Т. е. с учетом покрытия расходов.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»

Примечания — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

Библиография

[1] ISO/IEC 27001:2013, Information technology — Security techniques — Requirements of information security management systems

[2] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[3] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance

[4] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[5] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

[6] ISO/IEC 27006:2011, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[7] ISO/IEC 27007:2011, Information technology — Security techniques — Guidelines for information security management systems auditing

[8] ISO/IEC 27014:2013, Information technology — Security techniques — Governance of information security

[9] ISO 31000:2009, Risk management — Principles and guidelines

УДК 006.34:004:006.354 ОКС 35.040

Ключевые слова: система менеджмента информационной безопасности, информационная безопасность, менеджмент информационной безопасности, экономика информационной безопасности организации

Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 21.05.2021. Подписано в печать 08.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,55.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru