Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 10 (125)/2003

Информационная безопасность: экономические аспекты

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Введение

Отечественный ИТ-рынок в последние несколько лет динамично развивается, по оценкам экспертов его рост превышает 10% в год. При этом сектор информационной безопасности (ИБ) развивается еще более быстрыми темпами — более чем на 25% в год. Такой рост определяется в основном двумя факторами: возросшим вниманием руководства к обеспечению ИБ и недостаточным уровнем ИБ в существующих информационных системах (ИС).

Понятно, что долго такие темпы роста сектора ИБ сохраняться не смогут, они замедлятся, и вопросы оценки эффективности затрат в области ИБ встанут весьма остро. Уже сейчас в отечественных ИС с повышенными требованиями в области ИБ (банковские системы, ответственные производства, и т.д.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ. Даже в тех ИС, уровень ИБ которых явно не достаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством (владельцами информационных ресурсов) затрат на повышение этого уровня.

Начальники служб автоматизации, исполнительные директора, начальники служб информационной безопасности должны иметь понятные для бизнеса аргументы для обоснования инвестиций в ИБ, т.е., по сути, представлять обоснование стоимости системы ИБ для бизнеса.

В обосновании затрат на ИБ существует два основных подхода.

Первый подход, назовем его **наукообразным**, заключается в том, чтобы освоить, а затем и применить на практике необходимый инструментарий измерения уровня ИБ. Для этого необходимо привлечь руководство компании (как ее собственника) к оценке стоимости информационных ресурсов, определению оценки потенциального ущерба от нарушений в области ИБ. От результатов этих оценок будет во многом зависеть дальнейшая деятельность руководителей в области ИБ. Если информация ничего не стоит, существенных угроз для информационных активов компании нет, а потенциальный ущерб минимален (руководство это **подтверждает** (!)), проблемой обеспечения ИБ можно не заниматься. Если информация обладает определенной стоимостью, угрозы и потенциальный ущерб ясны, тогда встает вопрос о внесении в бюджет расходов на подсистему ИБ. В этом случае становится необходимым заручиться поддержкой руководства компании в осознании проблем ИБ и построении корпоративной системы защиты информации.

Второй подход, назовем его **практическим**, состоит в следующем: можно попытаться найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования оценка стоимости этой услуги составляет — 5-15% от рыночной стоимости автомобиля в зависимости от локальных условий его эксплуатации, стажа водителя, интенсивности движения, состояния дорог и т.д.

По аналогии, ИБ в компании можно вообще не заниматься, и не исключен такой вариант, что принятый риск себя вполне оправдает. А можно потратить на создание корпоративной системы защиты информации немало денег, и при этом останется некоторая уязвимость, которая рано или поздно приведет к утечке или хищению конфиденциальной информации.

Эксперты-практики в области защиты информации нашли некое оптимальное решение, при котором можно чувствовать себя относительно уверенно — стоимость системы ИБ должна составлять примерно 10-20% от стоимости КИС, в зависимости от конкретных требований к режиму информационной безопасности. Это и есть та самая оценка на основе практического опыта (best practice), которой можно уверенно оперировать, если не производить детальные расчеты.

Этот подход, очевидно, не лишен недостатков. В данном случае, скорее всего, не удастся вовлечь руководство в глубокое осознание проблем ИБ. Но зато можно обосновать объем бюджета на ИБ путем ссылки на понятные большинству владельцев информационных ресурсов общепринятые требования к обеспечению режима информационной безопасности «best practice», формализованные в ряде стандартов, например ISO 17799.

Реализация этих подходов (конкретные методы оценки эффективности системы ИБ) на практике зависит от ряда факторов, среди которых основными являются степень зрелости организации и специфика ее деятельности.

В статье рассматривается одна из наиболее известных методик оценки совокупной стоимости владения (ССВ) компании **Gartner Group** применительно к системе ИБ [1], [2], особеннос-

ти использования этой методики в отечественных условиях. Эта методика применима в случаях, когда используется первый подход к обоснованию затрат на ИБ.

2. Методика оценки совокупной стоимости владения для подсистемы ИБ

2.1 Возможности методики

Методика совокупной стоимости владения (ССВ) была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987) для оценки затрат на информационные технологии. Методика Gartner Group позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Данная методика может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы ИБ. Поскольку оценка экономической эффективности корпоративной системы защиты информации становится «измеримой», появляется возможность оперативно решать задачи контроля и коррекции показателей экономической эффективности и, в частности, показателя ССВ. Таким образом, показатель ССВ можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности КИС и обоснование бюджета на ИБ. При этом в компании эти работы могут выполняться самостоятельно, с привлечением системных интеграторов в области защиты информации или совместно предприятием и интегратором.

В целом методика ССВ компании Gartner Group позволяет:

- Получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации.
- Сравнить подразделения службы ИБ компании, как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли.
- Оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ССВ.

Показатель ССВ может использоваться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и позволяет «навести порядок» в существующих и планируемых затратах на ИБ. С этой точки зрения показатель ССВ дает возможность объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. Для объективности решения также необходимо дополнительно учитывать состояние внешней и внутренней среды предприятия, например, показатели технологического, кадрового и финансового развития предприятия, так как не всегда наименьший показатель ССВ корпоративной системы защиты информации может быть оптимален для компании.

Сравнение определенного показателя ССВ с аналогичными показателями ССВ по отрасли (с аналогичными компаниями) и с «лучшими в группе» позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто оказывается довольно трудно или даже практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же «родственных» показателей ССВ позволяет убедиться в том, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения можно проводить, используя усредненные показатели ССВ по отрасли, рассчитанные экспертами Gartner Group или собственными экспертами компании с помощью методов математической статистики и обработки наблюдений.

Методика ССВ Gartner Group позволяет ответить на следующие вопросы:

- Какие ресурсы и денежные средства расходуются на ИБ?
- Оптимальны ли затраты на ИБ для бизнеса компании?

- Насколько эффективна работа службы ИБ компании по сравнению с другими?
- Как эффективно управлять инвестированием в защиту информации?
- Какие выбрать направления развития корпоративной системы защиты информации?
- Как обосновать бюджет компании на ИБ?
- Как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом?
- Какова оптимальная структура службы ИБ компании?
- Как оценить эффективность нового проекта в области защиты информации?

2.2 Основные положения методики

ИБ обеспечивается комплексом мер на всех этапах жизненного цикла ИС, совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости:

- Проектных работ.
- Закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и AAA (средства аутентификации, авторизации и администрирования).
- Затрат на обеспечение физической безопасности.
- Обучения персонала.
- Управления и поддержки системы (администрирование безопасности).
- Аудита ИБ.
- Периодической модернизации системы ИБ.

Под показателем ССВ понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течении года. ССВ может рассматриваться как ключевой количественный показатель эффективности организации ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

При этом *прямые затраты* включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей и др., связанные с поддержкой деятельности организации.

В свою очередь *косвенные затраты* отражают влияние КИС и подсистемы защиты информации на сотрудников компании посредством таких измеримых показателей как простои и «зависания» корпоративной системы защиты информации и КИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам). Очень часто косвенные затраты играют значительную роль, так как они обычно изначально не отражаются в бюджете на ИБ, а выявляются явно при анализе затрат в последствии, что в конечном счете приводит к росту «скрытых» затрат компании на ИБ.

Существенно, что ССВ не только отражает «стоимость владения» отдельных элементов и связей корпоративной системы защиты информации в течение их жизненного цикла. «Овладение методикой» ССВ помогает службе ИБ лучше измерять, управлять и снижать затраты и/или улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании.

Подход к оценке ССВ базируется на результатах аудита структуры и поведения корпоративной системы защиты информации и КИС в целом, включая действия сотрудников служб автоматизации, информационной безопасности и просто пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения с аналогичными компаниями по отрасли.

Методика ССВ позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно: «сейчас мы тратим на ИБ столько-то, если будем тратить столько-то по конкретным направлениям ИБ, то получим такой-то эффект».

В методике ССВ в качестве базы для сравнения используются данные и показатели ССВ для западных компаний. Однако данная методика способна учитывать специфику российских компаний с помощью, так называемых, поправочных коэффициентов, например:

- По стоимости основных компонентов корпоративной системы защиты информации и

КИС, информационных активов компании с учетом данных по количеству и типам средств вычислительной техники, периферии и сетевого оборудования.
- По заработанной плате сотрудников с учетом дохода компании, географического положения, типа производства и размещения организации (крупный город или нет).
- По конечным пользователям ИТ с учетом типов пользователей и их размещения (для каждого типа пользователей требуется различная организация службы поддержки и вычислительной инфраструктуры).
- По использованию методов, так называемой, "лучшей практики" (best practice) в области управления ИБ с учетом реального состояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами.
- По уровню сложности используемой информационной технологии и ее интеграции в производственный процесс организации (процент влияния – до 40%).

В целом определение затрат компании на ИБ подразумевает решение следующих трех задач:
- Оценка текущего уровня ССВ корпоративной системы защиты информации и КИС в целом.
- Аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня ССВ.
- Формирование целевой модели ССВ.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ССВ

В ходе работ по оценке ССВ проводится сбор информации и расчет показателей ССВ организации по следующим направлениям:
- Существующие компоненты КИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства).
- Существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация).
- Существующие расходы на организацию ИБ в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.).
- Существующие расходы на организационные меры защиты информации.
- Существующие косвенные расходы на организацию ИБ в компании и, в частности, обеспечение непрерывности или устойчивости бизнеса компании.

Аудит ИБ компании

По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов:
- Политики безопасности.
- Организационных вопросов управления подсистемой безопасности.
- Классификации и управления информационными ресурсами.
- Управления персоналом.
- Физической безопасности.
- Администрирования компьютерных систем и сетей.
- Управления доступом к системам.
- Разработки и сопровождения систем.
- Планирования бесперебойной работы организации.
- Проверки системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ССВ, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя ССВ проверяемой компании с модельным значением показателя ССВ позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение «узких» мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

Формирование целевой модели ССВ

По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы "лучшей практики", типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации могут быть использованы модельные характеристики снижения совокупных затрат, отражающие возможные изменения в корпоративной системе защиты информации.

2.3 Границы применимости методики

Постановка задачи анализа эффективности инвестиций в обеспечение ИБ зависит от уровня зрелости организации. В [3] рассмотрена возможная классификация организаций по уровням зрелости:

- «Анархия».
- «Фольклор».
- «Стандарты».
- «Измеримый».
- «Оптимизируемый».

и их характеристика в области ИБ. Понятно, что подобная методика может эффективно применяться в организациях последних двух уровней зрелости («Измеримый», «Оптимизируемый»), частично быть полезной при уровне зрелости «Стандарты» и бесполезна на первых двух уровнях.

При применении экономических методов анализа эффективности инвестиций в ИБ для аргументации принятия тех или иных решений, необходимо помнить, что существуют и другие «неэкономические» факторы, в частности:

- Структура организации и особенности системы управления.
- Осведомленность и вовлеченность руководства в вопросы развития ИТ.
- Особенности стратегии организации.
- Позиции руководства отделов ИТ и ИБ в компании.
- Роль ИТ в производственном процессе.
- Случившиеся инциденты в области ИБ с тяжелыми последствиями.

Эти и возможно другие факторы следует учитывать наряду с экономическими при составлении аналитических материалов.

2.4 Пример оценки затрат на ИБ

В качестве примера использования методики ССВ для обоснования инвестиций в ИБ рассмотрим проект модернизации корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации (физическая защита).

Для этого сначала условно определим три возможных состояния системы защиты КИС от вирусов и вредоносного ПО, а именно: базовое, среднее и высокое.

Базовое: Стационарные и мобильные рабочие станции обладают локальной защитой от вирусов. Антивирусное программное обеспечение и базы сигнатур регулярно обновляются для успешного распознавания и парирования новых вирусов. Установлена программа автоматического уничтожения наиболее опасных вирусов. Основная цель уровня — организация минимальной защиты от вирусов и вредоносного ПО при небольших затратах.

Среднее: Установлена сетевая программа обнаружения вирусов. Управление программными обновлениями на сервере автоматизировано. Системный контроль над событиями оповещает о случаях появления вирусов и предоставляет информацию по предотвращению дальнейшего распространения вирусов. Превентивная защита от вирусов предполагает выработку и следование определенной политики защиты информации, передаваемой по открытым каналам связи Интернет. Дополнительно к техническим мерам используются организационные меры защиты информации.

Высокое: Антивирусная защита воспринимается как один из основных компонентов корпоративной системы защиты. Система антивирусной защиты тесно интегрирована в комплексную систему централизованного управления ИБ компании и обладает максимальной степенью автоматизации. При этом организационные меры по защите информации преобладают над техническими мерами. Стратегия защиты информации определяется исключительно стратегией развития бизнеса компании.

Также условно выделим три состояния развития системы контроля и управления досту-

пом в КИС (обеспечение физической безопасности): базовое, среднее, высокое.

Базовое: Ведется учет как минимум рабочих станций и серверов, инвентаризационные таблички крепятся на соответствующее аппаратное обеспечение. Введена процедура контроля перемещения аппаратных средств КИС. Проводятся постоянные и периодические инструктажи персонала компании. Особое внимание уделяется мобильным компонентам КИС.

Среднее: Используются механические и электронные замки, шлюзовые кабины и турникеты. Организованы контрольно-пропускные пункты и проходные. Осуществляется видеонаблюдение на объекте информатизации. Требования к персоналу определены и доведены под роспись. Разработаны инструкции по действию в штатных и внештатных ситуациях. Задействованы частные и государственные охранные предприятия и структуры.

Высокое: Обеспечение физической безопасности аппаратных средств является частью единой политики безопасности, утвержденной руководством компании. Активно используются весь комплекс мер защиты информации, начиная с организационного и заканчивая техническим уровнями.

Проект по модернизации корпоративной системы в части ИБ предполагает модернизацию двух элементов: антивирусной защиты и системы управления ИБ. Необходимо обосновать переход от базового уровня к повышенному (среднему или высокому). В табл. 1 приводятся требования к элементам защиты, сформулированные в задании на модернизацию КИС.

Возможно несколько вариантов реализации этих требований, характеризующихся разными экономическими показателями. Рассмотрим типичную структуру расходов по выбранным элементам системы ИБ «среднего западного» предприятия на модернизацию ИС (табл.2) для обеспечении «среднего» уровня защиты.

В табл. 3 и на рис. 1 показаны расчеты совокупной стоимости владения при различных вариантах проведения модернизации КИС. Данные приводятся для «среднего западного» предприятия. Расчетная стоимость снижения ССВ для третьего варианта около 230 тыс. долл. в год позволяют обосновать инвестиции в размере около 600 тыс. долл. на рассматриваемые компоненты защиты. При этом расчетный период окупаемости составляет не более 3 лет.

Расходы на аппаратные средства и программное обеспечение. Эта категория модели ССВ включает серверы, компьютеры клиентов (настольные и мобильные компьютеры), периферийные устройства и сетевые компоненты.

Элемент системы ИБ	Задача	Исходный (базовый) уровень	Повышенный уровень
Антивирусная защита	Каким образом распространяются обновления механизма антивирусной защиты?	Ничего не делается или нет информации	Используется автоматическое обновление антивирусного обеспечения
Антивирусная защита	Какая степень защиты от вирусов является допустимой?	Нет механизма защиты от вирусов	Защита от вирусов устанавливается ИС службой и не доступна пользователям для изменений
Антивирусная защита	Какой процент клиентских мест поддерживается серверной антивирусной защитой?	Нет данных	100 %
Антивирусная защита	Как устраняются последствия вирусных атак (в процентном отношении к числу вирусных событий)?	Пользователь самостоятельно восстанавливает поврежденные файлы и систему, протокол событий не ведется	ИС персонал уведомляется об инциденте, проводятся исследования и предпринимаются нейтрализующие меры, на местах поддерживается БД вирусных событий
Управление ИБ	Что делается для гарантии безопасности критичных данных (информация, которая является критичной по отношению к миссии каждого отдельного предприятия)	Не регламентирован	Средства шифрования и резервного копирования на серверах
Управление ИБ	Что делается для гарантии физической безопасности помещений с целью предотвращения случаев воровства и преступного использования оборудования?	Применяются сигналы тревоги о нарушении безопасности	Дополнительное использование таких средств безопасности, как смарт-карты или биометрические устройства

Табл. 1. Характеристики исходного и повышенного уровня защиты

Статья затрат	Антивирусная защита	Управление ИБ
Подготовительные процедуры и операции по инсталляции		
Услуги по инсталляции ПО:		
С учетом поддержки уровня 2	2,600 %	0,000 %
С учетом поддержки уровня 3	1,300 %	0,000 %
Администрирование пользователей	0,000 %	6,500 %
Установка аппаратного обеспечения	0,000 %	2,600 %
Резервное копирование, архивирование и восстановление	2,600 %	0,000 %
Планирование и управление процессами восстановления		
Общие процедуры управления, планирование и изучение рынка продуктов	1,300 %	1,300 %
Закупка программно-технических средств	18,200 %	2,600 %
Процедуры по восстановлению	19,500 %	0,000 %
Сервисное обслуживание		
Ежедневные процедуры поддержки пользователей	5,200 %	2,600 %
Административные расходы		
Финансовые службы и администрация	1,268 %	0,618 %
Административная поддержка ИС	0,429 %	0,169 %
Закупка, снабжение	0,000 %	5,200 %
Аудит	0,000 %	1,300 %
Управление контрактами, работа с поставщиками	0,000 %	2,600 %
Затраты рабочего времени конечных пользователей на решение задач ИБ		
Затраты времени на управление файлами, данными и резервным копированием	6,500 %	0,000 %
Затрата на взаимодействие со службами поддержки	6,500 %	0,000 %
Затрата на взаимопомощь пользователей	6,500 %	0,000 %
Затраты на самоподдержку (решение проблем своими силами)	6,500 %	2,600 %
Незапланированные простои по причинам, относящимся к данным средствам защиты	10,400 %	10,400 %

Табл. 2. Статьи расходов среднего уровня защиты.

Также в эту категорию входят расходы на аппаратно-программные средства ИБ.

Расходы на операции ИС. Прямые затраты на содержание персонала, стоимость работ и аутсорсинг, произведенные компанией в целом, бизнес-подразделениями или ИС службой для осуществления технической поддержки и операций по поддержанию инфраструктуры для пользователей распределенных вычислений.

Административные расходы. Прямые затраты на персонал, обеспечение деятельности и расходы внутренних/внешних поставщиков (вендоров) на поддержку ИС операций, включающих управление, финансирование, приобретение и обучение ИС.

Расходы на операции конечных пользователей. Это затраты на самоподдержку конечных пользователей, а также на поддержку пользователями друг друга в противовес официальной поддержке ИТ. Затраты включают: самостоятельную поддержку, официальное обучение конечных пользователей, нерегулярное (неофициальное) обучение, самостоятельные приклад-

Расходы на ИТ	Базовый вариант защиты: Антивирусная защита – низкий уровень Управление ИБ – низкий уровень	Вариант 1: Антивирусная защита – средний уровень Управление ИБ – низкий уровень	Вариант 2: Антивирусная защита – низкий уровень Управление ИБ – средний уровень	Вариант 3: Антивирусная защита – средний уровень Управление ИБ – средний уровень
Совокупная стоимость владения (ССВ)	$14,905,090	$14,659,236	$14,796,746	$14,563,990
Расходы на СВТ и ПО	$9,183,334	$9,212,787	$9,211,699	$9,241,232
Расходы на операции ИС	$1,402,287	$1,376,061	$1,394,232	$1,368,450
Административные расходы	$426,758	$425,554	$423,952	$422,748
Расходы на операции конечных пользователей	$2,772,377	$2,636,870	$2,758,898	$2,624,287
Расходы, связанные с простоями	$1,120,334	$1,007,965	$1,007,965	$907,273

Табл. 3. Совокупная стоимость владения при проведении модернизации

ные разработки, поддержку локальной файловой системы.

Расходы на простои. Данная категория учитывает ежегодные потери производительности конечных пользователей от запланированных и незапланированных отключений сетевых ресурсов, включая клиентские компьютеры, совместно используемые серверы, принтеры, прикладные программы, коммуникационные ресурсы и ПО для связи. Для анализа фактической стоимости простоев, которые связаны с перебоями в работе сети и которые оказывают влияние на производительность, исходные данные получают из обзора по конечным пользователям. Рассматриваются только те простои, которые ведут к потерям в основной деятельности организации.

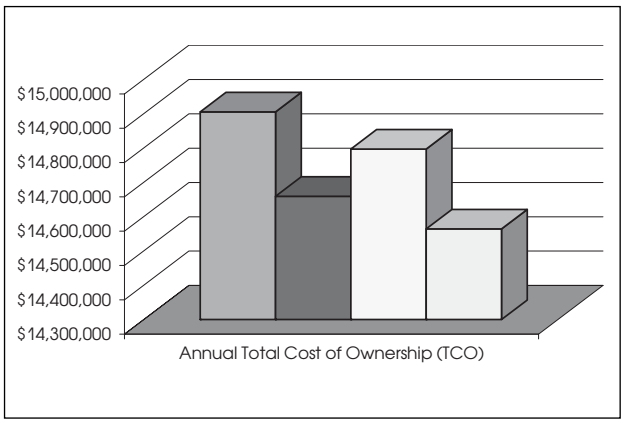

Рис. 1. Изменение ССВ при различных вариантах проведения модернизации системы ИБ

Отметим, что для применения методики ССВ требуются данные о потерях, связанных с простоями и другими негативными последствиях реализации угроз ИБ. Получить экономические оценки потерь можно на этапе анализа информационных рисков. Более подробно эти вопросы рассмотрены в [3], [4].

2.5 Разработка методик оценки затрат на ИБ

Рассмотрим, как можно определить прямые (бюджетные) и косвенные затраты на ИБ с учетом специфики российских компаний.

Предположим, что руководство компании проводит работы по внедрению на предприятии системы защиты информации (СЗИ). Уже определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые средства защиты информации. Для того, чтобы требуемый уровень защиты ресурсов реально достигался и соответствовал ожиданиям руководства предприятия, необходимо ответить на следующие основные вопросы, связанные с затратами на информационную безопасность:

- Что такое затраты на информационную безопасность?
- Неизбежны ли затраты на информационную безопасность?
- Какова зависимость между затратами на информационную безопасность и достигаемым уровнем информационной безопасности?
- Представляют ли затраты на информационную безопасность существенную часть от оборота компании?
- Какую пользу можно извлечь из анализа затрат на информационную безопасность?

Рассмотрим возможные ответы на поставленные вопросы.

Что такое затраты на информационную безопасность?

Как правило, затраты на информационную безопасность подразделяются на следующие категории:

- Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты).
- Затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия.
- Внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности (НПБ) — затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут.
- Внешние затраты на ликвидацию последствий нарушения политики информационной безопасности — компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.
- Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

При этом обычно выделяют *единовременные* и *систематические* затраты. К единовременным относятся затраты на формирование политики безопасности предприятия: организа-

ционные затраты и затраты на приобретение и установку средств защиты.

Классификация затрат условна, так как сбор, классификация и анализ затрат на информационную безопасность — внутренняя деятельность предприятий, и детальная разработка перечня зависят от особенностей конкретной организации. Самое главное при определении затрат на систему безопасности — взаимопонимание и согласие по статьям расходов внутри предприятия. Кроме того, категории затрат должны быть постоянными и не должны дублировать друг друга. Пример классификации затрат приводится в приложении 1.

Неизбежны ли затраты на информационную безопасность?

Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. Последние — это те, которые могут исчезнуть при отсутствии нарушений политики безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.

При соблюдении политики безопасности и проведении профилактики нарушений можно исключить или существенно уменьшить следующие затраты:

- На восстановление системы безопасности до соответствия требованиям политики безопасности.
- На восстановление ресурсов информационной среды предприятия.
- На переделки внутри системы безопасности.
- На юридические споры и выплаты компенсаций.
- На выявление причин нарушения политики безопасности.

Необходимые затраты — это те, которые необходимы даже если уровень угроз безопасности достаточно низкий. Это затраты на поддержание достигнутого уровня защищенности информационной среды предприятия.

Неизбежные затраты могут включать:

- Обслуживание технических средств защиты.
- Конфиденциальное делопроизводство.
- Функционирование и аудит системы безопасности.
- Минимальный уровень проверок и контроля с привлечением специализированных организаций.
- Обучение персонала методам информационной безопасности.

Какова зависимость между затратами на ИБ и уровнем защищенности КИС?

Сумма всех затрат на повышение уровня защищенности предприятия от угроз информационной безопасности составляет Общие затраты на безопасность.

Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия обычно имеет вид функции (рис. 2).

Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, затрат на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма — общие затраты на безопасность. Мы не включаем в данном случае единовременные затраты на формирование политики информационной безопасности предприятия, так как предполагаем, что такая политика уже выработана.

Снижение общих затрат

В примере (рис. 2) показано, что достигаемый уровень защищенности измеряется в категориях «большой риск» и «риск отсутствует» («совершенная защита»). Рассматривая левую сторону графика («большой риск»), мы видим, что общие затраты на безопасность высоки в основном потому, что высоки потери на компенсацию при нарушениях политики безопасности. Затраты на обслуживание системы безопасности очень малы.

Если мы будем двигаться вправо по графику, то достигаемый уровень защищенности будет увеличиваться (снижение информационного риска). Это происходит за счет увеличения объема предупредительных мероприятий, связанных с обслуживанием системы защиты. Затраты на компенсацию НПБ уменьшаются в результате предупредительных действий. Как показано на графике, на этой стадии затраты на потери падают быстрее, нежели возрастают за-

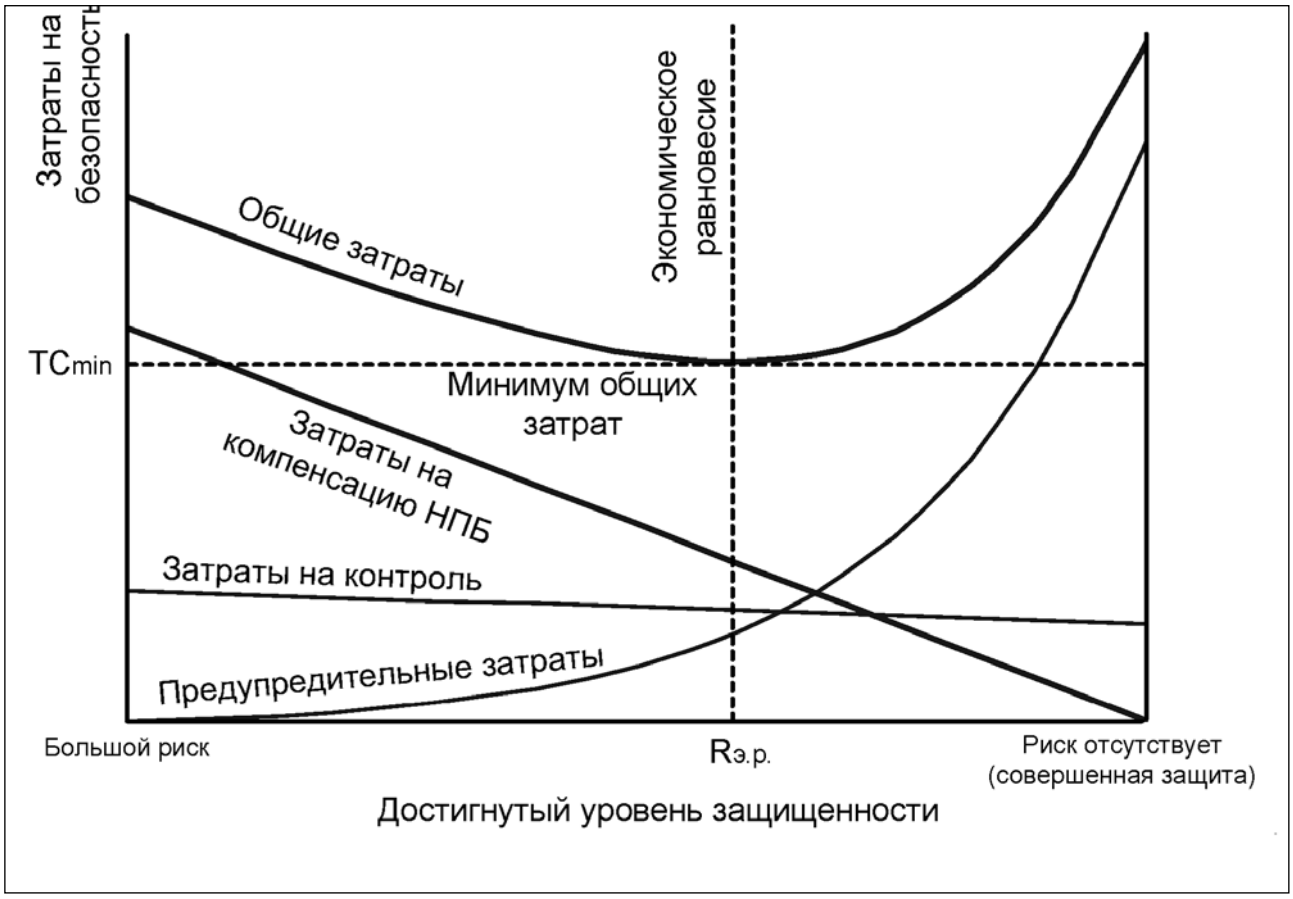

Рис.2. Взаимосвязь между затратами на безопасность и достигаемым уровнем защищенности

траты на предупредительные мероприятия. Как результат — общие затраты на безопасность уменьшаются. Изменения объема затрат на контроль незначительны.

Увеличение общих затрат

Если двигаться по графику вправо за точку экономического равновесия (т.е. достигаемый уровень защищенности увеличивается) ситуация начинает меняться. Добиваясь устойчивого снижения затрат на компенсацию нарушений политики безопасности, мы видим, что затраты на предупредительные мероприятия возрастают все быстрее и быстрее. Получается, что значительное количество средств должно быть затрачено на достижение достаточно малого снижения уровня риска.

График (рис. 2) отражает только общий случай, так как построен с учетом некоторых допущений, которые не всегда соответствуют реальным ситуациям.

Первое допущение заключается в том, что предупредительная деятельность по техническому обслуживанию комплекса программно-технических средств защиты информации и предупреждению нарушений политики безопасности предприятия соответствует следующему правилу: в первую очередь рассматриваются те проблемы, решение которых дает наибольший эффект по снижению информационного риска. Если не следовать этой модели, то вид графика станет совсем иным.

Второе допущение заключается в том, что точка экономического равновесия не изменяется во времени. На практике это допущение часто не выполняется. Основные факторы:

- Эффективность предупредительной деятельности не велика. В рассматриваемоей модели предполагается, что такая деятельность позволяет не повторять допущенные ранее ошибки. На практике это не так, и для достижения должного эффекта требуются гораздо большие затраты. В результате точка экономического равновесия сдвигается вправо.
- Устаревание системы ИБ.
- Разработчики средств защиты не успевают за активностью злоумышленников, которые

находят все новые и новые бреши в системах защиты. Кроме того, информатизация предприятия может породить новые проблемы, решение которых потребует дополнительных предупредительных затрат.

Все это может сместить экономическое равновесие по направлению к левому краю диаграммы.

Опасность ошибочной интерпретации

Многие руководители служб безопасности (СБ) предприятий уверены в том, что они работают на том уровне защищенности, который соответствует экономическому равновесию. Однако, как показывает практика, очень часто они не имеют веских доказательств для подтверждения этого предположения.

Рассмотренный график является идеализированным, на нем показан уровень защищенности информационной среды предприятия от угроз безопасности в терминах «высокий» и «низкий» и может не соотноситься с возможным ущербом.

Руководитель службы безопасности, который уверен, что он работает на базовом уровне защищенности, склонен верить, что это и есть экономическое равновесие, тогда как руководитель СБ, который думает, что он работает на максимальном уровне защищенности, верит, что экономическое равновесие находится именно на этом уровне.

Приведенный график может внушить таким руководителям СБ уверенность в том, что повышение защищенности информационной среды на их предприятиях будет сопровождаться лишь увеличением затрат. В результате никакой дополнительной деятельности в области ИБ вестись не будет.

Если предупредительные мероприятия проводятся должным образом и являются эффективными, то достаточно трудно найти доказательство того, что на каком-либо предприятии произошло повышение общих затрат на безопасность вследствие увеличения затрат на предупредительные мероприятия.

С другой стороны, если мы имеем дело с режимным объектом, который имеет очень низкий уровень риска, то есть теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик, то на таком объекте общие затраты на безопасность незначительны.

Оба эти факта могут привести некоторых к заключению, что данная концепция не работает.

Как оценить долю затрат на ИБ в обороте компании ?

Там, где затраты на обеспечение ИБ должным образом учтены, они могут составлять от 2 % до 20 % и более от объема продаж (оборота). Приведенная оценка получена из опыта работы российских компаний, специализирующихся в области защиты информации на основе анализа состояния защищенности информационной среды предприятий металлургической отрасли и отрасли связи.

Затраты на потери (внешние и внутренние)	=	70 % от общих затрат на безопасность
Затраты на контроль	=	25 % от общих затрат на безопасность
Затраты на предупредительные мероприятия	=	5 % от общих затрат на безопасность

Табл. 4. Типичное разделение затрат, связанных с ИБ

Предположим, что указанные затраты на безопасность составляют 10 % оборота. Далее предположим, что за счет увеличения объема предупредительных мероприятий и, следовательно, увеличения предупредительных затрат, удалось снизить общие затраты на безопасность до 6 % от оборота. Теперь распределение общих затрат на безопасность может быть следующее:

Затраты на потери (внешние и внутренние)	=	50 % от новой величины общих затрат на безопасность
Затраты на контроль	=	25 % от новой величины общих затрат на безопасность
Затраты на предупредительные мероприятия	=	25 % от новой величины общих затрат на безопасность

Табл. 5. Пример распределения общих затрат на безопасность

Однако общие затраты на обеспечение ИБ составили только 60% от их первоначальной величины.

По отношению к первоначальным общим затратам на ИБ, новое их распределение выглядит следующим образом:

Затраты на потери (внешние и внутренние)	50x60 / 100	=	30 % от начальной величины общих затрат на безопасность
Затраты на контроль	25x60 / 100	=	25 % от начальной величины общих затрат на безопасность
Затраты на предупредительные мероприятия	25x60 / 100	=	25 % от начальной величины общих затрат на безопасность
Экономия		=	**40 % от начальной величины общих затрат на безопасность**

Табл. 6. Пример соотношения распределения общих затрат на ИБ

При оценке затрат на систему безопасности на любом предприятии необходимо учитывать процентное соотношение общих затрат на безопасность и общего объема продаж.

3. Технология оценки затрат на ИБ

3.1 Как идентифицировать затраты на безопасность?

Первая задача — определить перечень затрат, которые относятся к деятельности предприятия и распределить их по категориям.

Вторая — составить перечень таким образом, чтобы смысл каждой позиции (каждого элемента) был ясен персоналу предприятия, и ввести ясную систему обозначения для каждой позиции перечня.

Общий смысл сбора данных по затратам на безопасность — обеспечить руководство предприятия инструментом управления.

Особенно важно, чтобы позиции перечня затрат были определимы в том виде, как они названы и распределены для различных категорий, в том числе:

- Для подразделения или какого-либо участка.
- Для защищаемого ресурса (по всем типам ресурсов).
- Для какого-либо рабочего места пользователя информационной среды предприятия.
- Для рисков по каждой категории информации.

Требования должны быть установлены самим предприятием для собственного (внутреннего) пользования. Однако при этом не следует забывать, что собранной информации должно быть достаточно для проведения последующего анализа.

Система защиты информации, а следовательно и система учета и анализа затрат на безопасность, которая не учитывает особенности предприятия, имеет слишком мало шансов на успех. Такая система должна быть встроена в организацию, как бы «сшита по мерке», ее нельзя взять уже готовую.

3.2 Как определить затраты на ИБ?

После того, как уже установлена система классификации и кодирования различных элементов затрат на безопасность, необходимо выявить источники данных о затратах. Такая информация уже может существовать, часть ее достаточно легко получить, в то время как другие данные определить будет значительно труднее, а некоторые могут быть недоступны.

Затраты на контроль

Элементы затрат на контроль приводятся в приложении 1. Основной объем затрат составляет оплата труда персонала службы безопасности и прочего персонала предприятия, занятого проверками и испытаниями. Эти затраты могут быть определены весьма точно. Оставшиеся затраты в основном связаны со стоимостью конкретных специальных работ и услуг внешних организаций и материально-техническим обеспечением системы безопасности. Они могут быть определены напрямую.

Итак, мы видим, что можно достаточно просто получить точную картину по затратам на контроль.

Внутренние затраты на компенсацию нарушений политики безопасности

Определение элементов затрат этой группы намного сложнее, но большую часть установить достаточно легко:

- Установка патчей или приобретение последних версий программных средств защиты информации.
- Приобретение технических средств взамен пришедших в негодность.
- Затраты на восстановление баз данных и прочих информационных массивов.

- Затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.
- Затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.

Труднее выявить объемы заработной платы и накладных расходов:

- По проведению дополнительных испытаний и проверок технологических информационных систем.
- По утилизации скомпрометированных ресурсов.
- По проведению повторных проверок и испытаний системы защиты информации.
- По проведению мероприятий по контролю достоверности данных, подвергшихся атаке на целостность.
- По проведению расследований нарушений политики безопасности.

Выяснение затрат на эти виды деятельности связаны с различными отделами:

- Отделом информационных технологий.
- Контрольно-ревизионным и финансовым отделами.
- Службой безопасности.

Поскольку каждый вовлеченный сотрудник вряд ли в течении всего рабочего дня решает проблемы, связанные только лишь с внутренними потерями от нарушений политики безопасности, оценка потерь должна быть произведена с учетом реально затраченного на эту деятельность времени. Таким образом, мы опять видим, что основные виды затрат в этой категории могут быть определены с достаточной степенью точности.

Внешние затраты на компенсацию нарушений политики безопасности

Часть внешних затрат на компенсацию нарушений политики безопасности связана с тем, что были скомпрометированы коммерческие данные партнеров и персональные данные пользователей услуг предприятия. Затраты, связанные с восстановлением доверия, определяются таким же образом, как и в случае внутренних потерь.

Однако существуют и другие затраты, которые определить достаточно сложно. В их числе:

- Затраты на проведение дополнительных исследований и разработку новой рыночной стратегии.
- Потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.
- Затраты, связанные с ликвидацией «узких мест» в снабжении, производстве и сбыте продукции.
- Потери от компрометации производимой предприятием продукции и снижения цен на нее.
- Возникновение трудностей в приобретении оборудования или технологий, в том числе повышение цен на них, ограничение объема поставок.

Перечисленные затраты могут быть вызваны действиями персонала различных отделов, например, проектного, технологического, планово-экономического, юридического, хозяйственного, отдела маркетинга, тарифной политики и ценообразования.

Поскольку сотрудники всех этих отделов вряд ли будут заняты полный рабочий день вопросами внешних потерь, то установление объема затрат необходимо вести с учетом реально затраченного времени.

Один из элементов внешних потерь невозможно точно вычислить — это потери, связанные с подрывом имиджа предприятия, снижением доверия потребителя к продукции и услугам предприятия. Именно по этой причине многие корпорации скрывают, что их сервис небезопасен. Корпорации боятся обнародования такой информации даже больше, чем атаки в той или иной форме. Однако многие предприятия игнорируют эти затраты на основании того, что их нельзя установить с какой-либо степенью точности — они только предположительны.

Затраты на предупредительные мероприятия

Эти затраты, вероятно, наиболее сложно оценить, поскольку предупредительные мероприятия проводятся в разных отделах и затрагивают многие службы. Эти затраты могут появляться на всех этапах жизненного цикла ресурсов информационной среды предприятия:

- Планирования и организации.
- Приобретения и ввода в действие.
- Доставки и поддержки.

- Мониторинга процессов, составляющих информационную технологию.

В дополнение к этому, большинство затрат данной категории связано с работой персонала службы безопасности. Затраты на предупредительные мероприятия в основном включают заработную плату и накладные расходы. Однако точность их определения в большей степени зависит от точности установления времени, затраченного каждым сотрудником в отдельности.

Некоторые предупредительные затраты легко выявить напрямую. Они, в частности, могут включать оплату различных работ сторонних организаций, например:

- Обслуживание и настройку программно-технических средств защиты, операционных систем и используемого сетевого оборудования.
- Проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.
- Доставку конфиденциальной информации.
- Консультации.
- Курсы обучения.

Источники сведений о затратах

При определении затрат на обеспечение ИБ необходимо помнить, что:

- Затраты на приобретение и ввод в действие программно-технических средств могут быть получены из анализа накладных, записей в складской документации и т. п..
- Выплаты персоналу могут быть взяты из ведомостей.
- Объемы выплат заработной платы должны быть взяты с учетом реально затраченного времени на проведение работ по обеспечению информационной безопасности. Если только часть времени сотрудника затрачивается на деятельность по обеспечению информационной безопасности, то целесообразность оценки каждой из составляющих затрат его времени не должна подвергаться сомнению.
- Классификация затрат на безопасность и распределение их по элементам должны стать частью повседневной работы внутри предприятия. С этой целью персоналу должны быть хорошо известны различные элементы затрат и соответствующие им коды.

Если все элементы собраны и распределены с достаточной точностью, то последующий анализ затрат на безопасность может вылиться лишь в интерпретацию данных.

Ответственность за сбор и анализ информации

Кто должен заниматься сбором и анализом данных, составлением отчета по затратам на безопасность? Это не может происходить от случая к случаю, необходима система. При этом надо быть уверенным в том, что все данные согласуются с финансовыми материалами, счетами и т. д. Кажется логичным привлечение экономистов к этой работе. Однако они будут нуждаться в помощи по классификации и анализу элементов затрат, а это уже работа Начальника службы безопасности.

Распределение деятельности и ответственности за нее может быть следующее (Таб.7).

Деятельность	Исполнитель
Определение категорий затрат	Экономический отдел и служба безопасности
Сбор данных о затратах	Экономический отдел
Распределение данных по категориям	Экономический отдел
Предоставление данных о затратах в службу безопасности	Экономический отдел
Анализ затрат	Служба безопасности
Исследование причин	Служба безопасности
Разработка рекомендаций по снижению затрат	Служба безопасности
Составление отчета по затратам на безопасность и его рассылка	Служба безопасности
Координация деятельности по управлению затратами внутри всего предприятия	Служба безопасности
Наблюдение за выполнением рекомендаций и корректирующих мероприятий	Служба безопасности

Табл. 7. Пример распределения деятельности и ответственности по затратам на ИБ

Данный список может быть изменен — каждая организация устанавливает свою собственную систему контроля и анализа затрат на безопасность.

База для сравнений

Затраты на безопасность, взятые сами по себе в абсолютном (стоимостном) выражении, могут привести к неверным выводам. Для иллюстрации сказанного рассмотрим пример. Предположим, что какая-либо организация получила общие затраты на безопасность за четыре периода подряд (в относительных единицах):

11 12 13 14

Эти данные, рассмотренные изолированно, приводят к выводу о том, что увеличение затрат на безопасность выходит из под контроля.

Тем не менее, если мы посмотрим объем производства за те же самые периоды времени, то обнаружим следующие величины:

100 120 140 160

Если теперь сравнить *общие затраты на безопасность*, отнесенные к *объему производства* за тот же период, то можно получить следующие данные:

12,5% 11% 10% 9,3%

Очевидно, что управление затратами на безопасность не ухудшалось по периодам, как это предполагалось первоначально, а скорее улучшалось. Хотя общие затраты на безопасность и увеличивались, объем производства увеличивался. Таким образом, *необходимо соотносить затраты на безопасность с какой-либо другой характеристикой деятельности, которая чувствительна к изменению производства.*

В рассмотренном выше примере, объем производства отражает, так называемую, *базу измерений*.

При определении отношения затрат на безопасность к какой-либо подходящей базе измерений важно быть уверенным, что период, для которого все эти характеристики определялись, был один и тот же.

Типовые базы измерений

Для многих организаций приемлемо будет соотносить затраты на безопасность *с объемом проданной продукции*, причем имеется в виду продукция, которая уже оплачена.

Однако, если объем продаж зависит от сезонных факторов или каких-либо других циклических изменений, объем проданной продукции не может быть достоверной базой, поскольку он будет слишком изменчив, в то время как объем производства и затраты на безопасность могут оставаться относительно постоянными. Необходимо отметить, что объем проданной продукции отличается от объема поставленной продукции, поскольку поставленная потребителю продукция может быть еще не оплачена. Точно также и объем произведенной продукции может не совпадать с объемом реально проданной или поставленной. Конечно же решение о том, с какой базой измерений соотносить затраты на безопасность — стоимостью произведенной продукции; числом произведенных единиц продукта; объемом проданной продукции; стоимостью поставленной продукции — должно быть принято самим предприятием. Руководство при этом должно быть уверено, что полученные результаты действительно отражают реальную и объективную картину затрат на безопасность.

Другие базы измерений

Ниже рассмотрены некоторые базы измерений и даны пояснения почему их рекомендуется использовать.

Трудоемкость

Трудоемкость может быть представлена как величина оплаты труда, непосредственно затраченного на производство продукции. Это часто используемая на практике финансовая категория, и поэтому данные для использования в этой базе измерений должны быть, безусловно, доступны. Однако трудоемкость должна использоваться с осторожностью, поскольку она может изменяться по различным причинам, например:

- Улучшение технологии.
- Автоматизация технологических процессов.
- Смена обслуживающего персонала.

Таким образом, трудоемкость как база измерений может быть использована только для коротких промежутков времени.

Важно помнить следующее:

- Трудоемкость не может быть использована в качестве измерительной базы в том случае, если не учитывается эффект инфляции.
- Необходимо всегда сравнивать величины в их стоимостном выражении.

Характерный пример использования данной базы: отношение внутренних затрат на компенсацию последствий нарушений политики безопасности к трудоемкости.

Определение ценности информационных ресурсов предприятия

Ценность информационных ресурсов предприятия с экономической точки зрения — это совокупная стоимость собственных ресурсов, выделяемых в информационной среде предприятия. Ресурсы обычно подразделяются на несколько классов, например, физические, программные и информационные (данные). Для каждого класса должна существовать своя методика оценки ценности.

Оценка ценности ресурсов проводится специализированными организациями во время выполнения работы по анализу рисков безопасности предприятия. Как правило, оценка физических ресурсов производится с учетом стоимости их замены или восстановления работоспособности. Программные ресурсы оцениваются тем же способом, что и физические — на основе определения затрат на их приобретение или восстановление. Если для информационного ресурса существуют особенные требования к конфиденциальности или целостности (например, если исходный текст имеет высокую коммерческую ценность), то оценка этого ресурса производится по той же схеме, то есть в стоимостном выражении.

При разработке конкретных методик оценки ССВ всегда надо помнить о "тонких" моментах, связанных с оценкой ценности информационных ресурсов, учетом последствий нарушения режима ИБ. Как правило имеются экономические и неэкономические аспекты (например, аспекты, связанные с разглашением персональной информации или потерей репутации организации). Последние надо приводить (отображать) в денежные шкалы, что обычно делается на этапе анализа рисков.

Таким образом, анализ информационных рисков является неотъемлимой частью подобных методик, комплекс этих вопросов подробно рассматривается в [4].

Оценка эффективности деятельности службы ИБ

Необходимо иметь достаточно простую систему оценки, позволяющую оценить деятельности службы ИБ в качественных шкалах в разные периоды времени. Например, может использоваться субъективная оценка вероятности серьезного происшествия в области ИБ, которую дают ведущие специалисты отдела ИБ.

Данные измерений	Вывод
0,0 – 0,1	Надежность защиты высокая
0,1 – 0,25	Появились проблемы в системе защиты
0,25 – 0,5	Необходимо усилить систему защиты информации
0,5 – 0,75	Необходимо менять политику безопасности

Табл. 8. Пример оценки вероятности серьезного происшествия в течение года

Данная таблица приведена в качестве примера, как можно использовать любые соотношения, которые помогут «рассортировать» интересующую нас информацию.

Целью использования всех рассмотренных соотношений является сравнение эффективности деятельности предприятия в различные периоды времени.

Анализ затрат на обеспечение ИБ

Отчет по затратам на безопасность

Результаты анализа затрат на безопасность и итоговый отчет должны показать объективную картину в отношении безопасности.

Анализ затрат на безопасность – инструмент управления, он используется руководством предприятия для определения достигнутого уровня защищенности информационной среды и обнаружения проблем при постановке задач по достижению требуемого уровня защищенности.

Представленный в финансовых терминах и составленный простым языком отчет по затратам на безопасность имеет значительные преимущества перед другими видами отчетов по исследованию безопасности информационной среды предприятия и анализу рисков.

Содержание отчета по затратам на безопасность в большей степени зависит от того, кому он предназначается и от того, какую роль играет в рамках предприятия тот, кому данный конкретный отчет предназначен.

Руководство должно получить краткий отчет, который предоставляет общую картину о состоянии системы безопасности предприятия. Отчет содержит финансовые термины, должен быть доступно написан и содержать только объективную информацию.

Руководители подразделений информатизации и защиты информации должны получить

Затраты	Периоды			
	I	II	III	IV
РЕСУРС "А"				
Предупредительные	227	198	209	251
На контроль	593	616	606	614
На внутренние потери	985	1016	758	744
На внешние потери	503	528	482	427
Общие затраты на безопасность	2308	2358	2065	2036
Общие затраты на безопасность, отнесенные к объему продаж	1.0 %	1,05 %	0,9 %	0,85 %
Общие затраты на безопасность, отнесенные к трудоемкости	1,9 %	2 %	1,5 %	1,4 %
РЕСУРС "В "				
Предупредительные	206	229	340	397
На контроль	894	949	916	925
На внутренние потери	1903	1935	1034	948
На внешние потери	620	598	613	632
Общие затраты на безопасность	3623	3711	2903	2902
Общие затраты на безопасность, отнесенные к объему продаж	1,1 %	1,15 %	0,9 %	0,9 %
Общие затраты на безопасность, отнесенные к трудоемкости	2,5 %	2,55 %	1,4 %	1,3 %
РЕСУРС "С"				
Предупредительные	184	242	299	347
На контроль	815	859	831	802
На внутренние потери	1187	1191	910	893
На внешние потери	1101	1066	72	568
Общие затраты на безопасность	3287	3358	2762	261
Общие затраты на безопасность, отнесенные к объему продаж	1,2 %	1,2 %	1,0 %	0,9 %
Общие затраты на безопасность, отнесенные к трудоемкости	1,9 %	1,9 %	1,5 %	1,4 %

Табл. 9. Отчет по затратам на безопасность (пример)

более детальную информацию о достигнутом уровне защищенности тех ресурсов информационной среды предприятия, за которые оно отвечает. Отчет должен быть очень подробным и представлять данные по типам ресурсов, видам угроз и т. д. Принципом проведения анализа затрат на безопасность является получение результатов в форме, наиболее полезной и удобной для тех, кому предназначен отчет.

Руководитель, читающий отчет, должен получить информацию, которая позволит:

- Сравнить текущий уровень защищенности с уровнем прошлого периода, то есть выявить тенденции.
- Сравнить текущий уровень с поставленными целями.
- Выявить наиболее значительные области затрат.
- Выбрать области для улучшения.
- Оценить эффективность программ по улучшению.

Руководитель ожидает получить отчет по затратам на безопасность, который:

- Расскажет ему о тех вещах, которые относятся лишь к его сфере компетенции и ничего более.
- Написан легким для понимания языком и не напичкан специальными терминами.
  Написан четко и кратко и содержит всю необходимую информацию.
- Позволяет определить первоочередные задачи и направления деятельности.

Отчет для руководителей подразделений информатизации и защиты информации может быть представлен в виде таблицы. Предположим, что составляется отчет за три информационных ресурса, например, «А», «В» и «С», которые различаются между собой только лишь видом содержащейся информации. Оценки стоимости ресурсов близкие, а технологии защиты схожи друг с другом. Например, отчет по затратам на безопасность может выглядеть следующим образом (табл. 9).

Код	Источник затрат	Угроза случайного или умышленного изменения информации		Угроза временной недоступности информации		Сумма (усл.ед.)	Доля (%)
		Сумма	Доля (%)	Сумма	Доля (%)		
W1	Восстановление системы защиты ресурса до соответствия требованиям ПБ	1001	89,3	120	10,7	1121	57,9
W2	Восстановление ресурса	133	100	-	-	133	6,9
W3	Выявление причин нарушения ПБ	97	87,4	14	12,6	111	5,7
W4	Изменения	440	77,2	130	32,8	570	29,5
	Итого:	1671		264		**1935**	**100**

Табл. 10. Составляющие затрат на внутренние потери

Механизмы защиты	Сумма (усл.ед.)	Доля (%)
Затраты на введение дополнительных мер, связанных с учетом подключений пользователей к ресурсу	133	13,29
Затраты на введение дополнительных мер, связанных с контролем прав доступа сотрудников и учетом изменений их состояния (увольнение, перевод, отпуск, продолжительная болезнь)	88	8,79
Затраты на установку системы передачи файлов отчетов на сервер протоколирования	280	27,97
Приобретение дополнительных модулей удаленных запросов и выборок администратором системы безопасности	500	49,95
ИТОГО:	**1001**	**100**

Табл. 11. Составляющие затрат на внутренние потери в следствие реализации угрозы целостности информации

Анализ затрат

Если проанализировать данные по I-му и II-му периодам, приведенные в табл. 9, то можно обнаружить, что чрезвычайно велики внутренние потери на компенсацию нарушений политики безопасности для ресурса «B», а также внешние потери на НПБ для ресурса «C».

Руководитель отдела защиты информации предпринял шаги в данном направлении. Он увеличил после II-го периода объем предупредительных мероприятий для ресурса «B», и это дало значительный эффект по снижению внутренних потерь на НПБ к концу III-го периода.

Он также увеличил после II-го периода предупредительную деятельность для ресурса «C», и после III-го периода так же произошло снижение внешних затрат на НПБ. Хотя предупредительные действия для этого ресурса не дали столь же быстрого результата, как для ресурса «B», тем не менее затраты были снижены, а к концу IV-го периода — даже в еще большей степени.

Однако, прежде чем проводить какие-либо мероприятия по усилению защищенности информационной среды предприятия, необходимо ответить на следующие вопросы: С чего надо начинать? В чем причина происходящего?

Начальнику отдела защиты информации необходима значительно большая информация, чем представленная в суммирующей таблице. Он знает, что у него возникли проблемы, но не знает какими причинами они вызваны. Он нуждается в более детальном дроблении элементов затрат на безопасность.

Итак, к концу II-го периода начальник отдела защиты информации получил следующую информацию, конкретизирующую внутренние затраты на НПБ по ресурсу «B» в зависимости от угроз безопасности ресурса (табл. 10).

Приведенные данные показывают, что наибольшие потери связаны с воздействием угрозы случайного или умышленного изменения информации и возникающей необходимостью восстановления системы защиты ресурса до соответствия требованиям политики безопасности. Более детальная информация показывает механизмы защиты, которые были использованы для усиления системы защиты ресурса (табл.11).

Анализ этих сведений помогает определить, что предупредительные мероприятия должны быть направлены, в первую очередь, на обеспечение соответствия требованиям качест-

ва информационных технологий, а во вторую — на решение проблемы аудита системы безопасности и т. д.

Прежде чем тратить средства на предупредительные мероприятия в области обеспечения качества информационной технологии, Начальник отдела защиты информации подробно и досконально рассматривает возможные причины нанесения ущерба (уязвимости технологии защиты ресурса), например такие:

- Недостаточные возможности по архивированию данных.
- Бессистемность проведения мероприятий по архивированию данных.
- Непригодность механизма учета и контроля носителей резервных копий.
- «Слабость» нормативной базы.
- Отсутствие практики проведения тестовых испытаний системы защиты ресурсов.
- Недостаточность технических систем охлаждения и питания серверных комнат.
- Отсутствие регламента программно-технических средств «типовой рабочей станции» и т. д.

Как оказалось, в нашем примере ни одна из перечисленных причин не составляет более чем 8% от общей величины потерь в рассматриваемый период. Однако затраты на минимизацию перечисленных потерь будут существенно различны в зависимости от решаемой проблемы: наименьшие в случае совершенствования нормативной базы и, возможно, весьма значительные при оборудовании серверных комнат техническими системами охлаждения и питания.

Принятие решений

Все выявленные причины нанесения ущерба заслуживают корректирующих мероприятий, однако руководитель осуществляет поиск тех областей, которые дадут наибольшую отдачу в ответ на затраченные усилия. Именно поэтому он может рассмотреть, как первоочередную для улучшения область своих затрат, связанную с внедрением системы передачи файлов отчетов на сервер протоколирования.

Тщательный анализ может привести начальника отдела защиты информации к выводу о том, что лучше начать предупредительные мероприятия для механизмов защиты, имеющих не самую большую затратную часть.

Без доступной детальной информации борьба за повышение уровня защищенности информационной среды предприятия будет равносильна борьбе с «огнем» вместо «предупреждения пожаров».

Итак, необходимо отметить следующее:

- *Затраты на безопасность могут быть снижены в значительной степени за счет того, что будут выявлены специфические причины потерь и предложены программы снижения уровня риска.*
- *Все рекомендации по улучшениям должны содержать данные о стоимости применения предложенных программ. Меры снижения уровня риска должны преследовать следующую цель: с наименьшими затратами получить наилучшие результаты.*

3.3 Внедрение системы учета затрат на ИБ

Все вышеизложенное может показаться сложным и трудоемким для реализации. Вероятно, в связи с этим на практике редко встретишь организации, внедрившие систему сбора и анализа затрат на безопасность.

Руководители системы безопасности должны быть убеждены в полезности этого мероприятия.

Ниже предложены некоторые «секреты» успешного внедрения системы.

- **Начинайте с малого и наращивайте.** Возьмитесь за простое, не пытайтесь сразу же охватить все ресурсы, требующие защиты. Выберите один вид ресурса — то, что вы хотите, и стройте систему, которую сможете наполнить фактическими финансовыми данными.

- **Создайте образец, чтобы показать, как это может быть сделано.** Начните с тех затрат на безопасность, для которых данные уже известны. Определите иные необходимые затраты «экспертным» способом, если это необходимо.

- **Не бойтесь препятствий и не откладывайте работу**, решив проблему один раз, вы облегчите себе жизнь в будущем.
- **Подтвердите документами ценность анализа затрат на ИБ.** Упростите систему так, чтобы она соответствовала потребностям Вашей организации.

Если затраты определены с точностью ±5%, то работа сделана с приемлемой точностью. Руководство предприятия получит более точную картину затрат на безопасность, а следовательно и оценку уровня риска.

Заключение

Вместе с методикой ССВ можно использовать разнообразные методы для расчета возврата инвестиций (ROI). Как правило, для оценки доходной части сначала анализируют те цели, задачи и направления бизнеса, которые нужно достигнуть с помощью внедрения или реорганизации существующих проектов в области системной интеграции, автоматизации и информационной безопасности. Далее используют некоторые измеримые показатели эффективности бизнеса для оценки отдельно по каждому решению. Указанные показатели не надо выдумывать, они существуют в избыточном виде. Далее можно использовать методики расчета *коэффициентов возврата инвестиций в инфраструктуру предприятия (ROI)*, например, Gartner Group.

По нашему мнению, достаточно результативно использовать следующую комбинацию: ССВ как расходную часть и ROI как расчетную. Кроме того, сегодня существуют и другие разнообразные методы и технологии расчета и измерения различных показателей экономической эффективности.

Приложение 1

Примерный перечень затрат организации на обеспечение ИБ

Предположим, что основы политики безопасности на предприятии сформированы. Систематические затраты на ИБ можно разбить на следующие группы.

Затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия)

Управление системой защиты информации:

- Затраты на планирование системы защиты информации предприятия.
- Затраты на изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения.
- Затраты на осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации.
- Проверка сотрудников на лояльность, выявление угроз безопасности.
- Организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой.

Регламентное обслуживание средств защиты информации:

- Затраты, связанные с обслуживанием и настройкой программно-технических средств защиты, операционных систем и используемого сетевого оборудования.
- Затраты, связанные с организацией сетевого взаимодействия и безопасного использования информационных систем.
- Затраты на поддержание системы резервного копирования и ведение архива данных.
- Проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.

Аудит системы безопасности:

- Затраты на контроль изменений состояния информационной среды предприятия.
- Затраты на систему контроля за действиями исполнителей.

Обеспечение должного качества информационных технологий:

- Затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации.
- Затраты на доставку (обмен) конфиденциальной информации.
- Удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.

Обеспечение требований стандартов:

- Затраты на обеспечение соответствия принятым стандартам и требованиям, достоверности информации, действенности средств защиты.

Обучение персонала:

- Повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности.
- Развитие нормативной базы службы безопасности.

Затраты на контроль:

- Плановые проверки и испытания.
- Затраты на проверки и испытания программно-технических средств защиты информации.
- Затраты на проверку навыков эксплуатации средств защиты персоналом предприятия.
- Затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям.
- Оплата работ по контролю правильности ввода данных в прикладные системы.
- Оплата инспекторов по контролю требований, предъявляемых к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований).

Внеплановые проверки и испытания:

- Оплата работы испытательного персонала специализированных организаций.
- Обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами.

Контроль за соблюдением политики ИБ:

- Затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны.
- Затраты на организацию временного взаимодействия и координации между подразделениями для решения повседневных конкретных задач.
- Затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия.
- Материально-техническое обеспечение системы контроля доступа к объектам и ресурсам предприятия.

Затраты на внешний аудит:

- Затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации.

Пересмотр политики информационной безопасности предприятия (проводится периодически):

- Затраты на идентификацию угроз безопасности.
- Затраты на поиск уязвимостей системы защиты информации.
- Оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска.

Затраты на ликвидацию последствий нарушения режима ИБ:

- Восстановление системы безопасности до соответствия требованиям политики безопасности.
- Установка патчей или приобретение последних версий программных средств защиты информации.
- Приобретение технических средств взамен пришедших в негодность.
- Проведение дополнительных испытаний и проверок технологических информационных систем.
- Затраты на утилизацию скомпрометированных ресурсов.

Восстановление информационных ресурсов предприятия:

- Затраты на восстановление баз данных и прочих информационных массивов.
- Затраты на проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность.

Затраты на выявление причин нарушения политики безопасности:

- Затраты на проведение расследований нарушений политики безопасности (сбор данных о способах совершения, механизме и способах сокрытия неправомерного деяния. поиск следов, орудий и предметов посягательства; выявление мотивов неправомерных действий и т. д.).
- Затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.

Затраты на переделки:

- Затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.
- Затраты на повторные проверки и испытания системы защиты информации.

Внешние затраты на ликвидацию последствий нарушения политики безопасности:

- Обязательства перед государством и партнерами.
- Затраты на юридические споры и выплаты компенсаций.
- Потери в результате разрыва деловых отношений с партнерами.

Потеря новаторства:

- Затраты на проведение дополнительных исследований и разработки новой рыночной стратегии.
- Отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений и затраты на разработку новых средств ведения конкурентной борьбы.
- Потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

Прочие затраты:

- Заработная плата секретарей и служащих, организационные и прочие расходы, которые непосредственно связаны с предупредительными мероприятиями.
- Другие виды возможного ущерба предприятию, в том числе связанные с невозможностью выполнения функциональных задач, определенных его Уставом.

Литература

1. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A. Weintraub, V. Wheatman. The Price of Information Security. Gartner Research, Strategic Analysis Report, K-11-6534, June 2001.
2. R. Witty. The Role of the Chief Information Security Officer. Research Note, Gartner Research, Strategic Planning, SPA-13-2933, April 2001.
3. Симонов С.В. Технологии и инструментарий для управления рисками М.: Jet Info № 2, 2003.
4. Петренко С.А. Симонов С.В. Экономически оправданная безопасность. Управление информационными рисками. Изд. ДМК, Москва, 2003.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем