Оценка затрат на кибербезопасность

С. А. Петренко

Сегодня в отечественных компаниях и предприятиях с повышенными требованиями в области информационной безопасности (государственные, банковские системы, билинговые системы, ответственные производства и т. д.) затраты на обеспечение режима информационной безопасности (ИБ) составляют до 30 % всех затрат на информационную систему (ИС), и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ. Даже в тех ИС, уровень ИБ которых явно недостаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством предприятий и организаций затрат на повышение этого уровня. Как определить экономически оправданные затраты на защиту информации? Какие методы существуют и жизнеспособны на практике? Давайте посмотрим вместе.

Обзор существующих методов

Первоначально определимся с целями, которые мы преследуем при выборе метода оценки целесообразности затрат на систему информационной безопасности. Во-первых, метод должен обеспечивать количественную оценку затрат на безопасность, используя качественные показатели оценки вероятностей событий и их последствий. Во-вторых, метод должен быть прозрачен с точки зрения пользователя и давать возможность вводить собственные эмпирические данные. В-третьих, метод должен быть универсален, т. е. одинаково применим к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, затрат на перемещение персонала и обучение конечных пользователей и т. д. В-четвертых, выбранный метод должен позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия. Давайте посмотрим, какие методы оценки затрат и ценности инвестиций существуют и что можно использовать на практике.

Прикладной информационный анализ — Applied Information Economics (AIE)

Методика Applied Information Economics (AIE) была разработана Дугласом Хаббардом, руководителем компании Hubbard Ross. Компания Hubbard Ross, основанная в марте 1999 г., стала первой организацией, которая использовала методику AIE для анализа ценности инвестиций в технологии безопасности с финансовой и экономической точки зрения.

Методика AIE позволяет повысить точность показателя «действительная экономическая стоимость вложений в технологии безопасности» за счет определения доходности инвестиций (Return on Investment, ROI) до и после инвестирования. Применение AIE позволяет сократить неопределенность затрат, рисков и выгод, в том числе и неочевидных. Опираясь на знания экономики, статистики, теории информации и системного анализа, консультанты Hubbard Ross определяют важные финансовые показатели, используя дополнительные сведения для уменьшения их неопределенности, также оценивают влияние рисков и помогают выбрать такую стратегию, которая уменьшала бы риск и оптимизировала инвестиционные вложения.

Отчет о проделанной работе включает в себя полученные сведения, рекомендации и комментарии консультантов, также в состав отчета входит сводная таблица, сделанная с помощью Microsoft Excel, отражающая взаимное влияние затрат, прибыли и рисков.

Потребительский индекс — Customer Index (CI)

Метод предлагает оценивать степень влияния инвестиций в технологии безопасности на численность и состав потребителей. В процессе оценки предприятие или организация определяет экономические показатели своих потребителей за счет отслеживания доходов, затрат и прибылей по каждому заказчику в отдельности. Недостаток метода состоит в трудности формализации процесса установления прямой связи между инвестициями в технологии безопасности и сохранением или увеличением числа потребителей. Этот метод применяется в основном для оценки эффективности корпоративных систем защиты информации в компаниях, у которых число заказчиков непосредственно влияет на все аспекты бизнеса.

Добавленная экономическая стоимость — Economic Value Added (EVA)

Консалтинговая компания Stern Stewart и Co., основанная в 1982 г., специализируется на оценке акционерного капитала новым инструментарием финансового анализа. Эта компания, одна из первых, разработала собственную методику вычисления добавленной стоимости (Economic

Value Added), которая предлагает непротиворечивый подход к определению целей и измерению показателей, к оценке стратегий, к размещению капитала и пр.

Методика EVA предлагает рассматривать службу информационной безопасности как «государство в государстве», т. е. специалисты службы безопасности продают свои услуги внутри компании по расценкам, примерно эквивалентным расценкам на внешнем рынке, что позволяет компании отследить доходы и расходы, связанные с технологиями безопасности. Таким образом, служба безопасности превращается в центр прибыли и появляется возможность четко определить, как расходуются активы, связанные с технологиями безопасности, и увеличиваются доходы акционеров.

Исходная экономическая стоимость — Economic Value Sourced (EVS)

Методика EVS была разработана компанией META Group Consulting, которая оказывает услуги средним и крупным компаниям, количественно измеряя возврат от инвестиций в технологии безопасности. Методика предполагает точный расчет всех возможных рисков и выгод для бизнеса, связанных с внедрением и функционированием корпоративной системы защиты информации. При этом расширяется использование таких инструментальных средств оценки ИТ, как добавленная экономическая стоимость (EVA), внутренняя норма рентабельности (IRR) и возврат от инвестиций (ROI), за счет определения и вовлечения в оценочный процесс параметров времени и риска.

Управление портфелем активов — Portfolio Management (PM)

Методика управления портфелем активов предполагает, что компании управляют технологиями безопасности так же, как управляли бы акционерным инвестиционным фондом с учетом объема, размера, срока, прибыльности и риска каждой инвестиции. Портфель активов технологий безопасности состоит из «статичных» активов и «динамичных» активов. К «статическим» активам относят: аппаратно-программные средства защиты информации, операционные системы и пакеты прикладных программных продуктов, сетевое оборудование и программное обеспечение, данные и информацию, оказываемые услуги, человеческие ресурсы и прочее. В состав «динамичных» активов входят следующие компоненты — это различные проекты по расширению и обновлению всего портфеля активов, знания и опыт, интеллектуальный капитал и т. д.

Таким образом, управление портфелем активов технологий безопасности представляет собой непрерывный анализ взаимодействия возникающих возможностей и имеющихся в наличии ресурсов. Непрерывность процесса управления связана с внешними изменениями (например, изменение ситуации на рынке, изменение позиций конкурента) и с внутренними изменениями (например, изменение в стратегии компании, в каналах сбыта, номенклатуре товаров и услуг и т. д.). А директор службы безопасности становится «фондовым менеджером», который управляет инвестициями в технологии безопасности, стремясь к максимизации прибыли.

Оценка действительных возможностей Real Option Valuation (ROV)

Основу методики составляет ключевая концепция построения модели «гибких возможностей компании» в будущем. Методика рассматривает технологии безопасности в качестве набора возможностей с большой степенью их детализации. Правильное решение принимается после тщательного анализа широкого спектра показателей и рассмотрения множества результатов или вариантов будущих сценариев, которые в терминах методики именуются «динамическим планом выпуска» управляющих решений или гибкости, который поможет организациям лучше адаптировать или изменять свой курс в области информационной безопасности.

Метод жизненного цикла искусственных систем — System Life Cycle Analysis (SLCA)

В основе российского метода жизненного цикла искусственных систем System Life Cycle Analysis (SLCA) лежит измерение «идеальности» корпоративной системы защиты информации — соотношение ее полезных факторов к сумме вредных факторов и факторов расплаты за выполнение полезных функций. Оценку предваряет совместная работа аналитика и ведущих специалистов обследуемой компании по выработке реестра полезных, негативных и затратных факторов бизнес-системы без использования системы безопасности и присвоению им определенных весовых коэффициентов. Результатом работы является расчетная модель, описывающая состояние без системы безопасности. После этого в модель вводятся описанные факторы ожидаемых изменений, и производится расчет уровня развития компании с корпоративной системой защиты информации. Таким образом, строятся традиционные модели «Как есть» и «Как будет» с учетом реестра полезных, негативных и затратных факторов бизнес-системы.

Данный метод SLCA применяется:

1) на этапе предпроектной подготовки, для предварительной оценки эффекта от внедрения новой системы безопасности или от модернизации существующей;
2) на этапе разработки технического задания на АС в защищенном исполнении;
3) на этапе проведения аудита информационной безопасности АС предприятия, для проектной оценки ожидаемого эффекта;
4) на этапе приемки АС в защищенном исполнении в эксплуатацию или по окончанию периода опытной эксплуатации для подтверждения расчетного эффекта, его уточнения и получения новой «точки отсчета» (нового уровня организационно-технологического развития компании) для последующих оценок эффекта от внедрения технологий безопасности.

Система сбалансированных показателей — Balanced Scorecard (BSC)

Balanced Scorecard (Система сбалансированных показателей (ССП)) — это методика, в рамках которой традиционные показатели финансовых отчетов объединяются с операционными параметрами, что создает достаточно общую схему, позволяющую оценить нематериальные активы: уровень корпоративных инноваций, степень удовлетворенности сотрудников, эффективность приложений и т. д.

Концепция системы сбалансированных показателей впервые была представлена в 1990 г. Дэвидом Нортоном, на сегодняшний день руководителем Balanced Scorecard Collaborative, и Робертом Капланом, профессором Harvard Business School. Традиционная концепция ССП предполагает формирование так называемых стратегических карт, группирующих цели и показатели по четырем категориям (перспективам):

- Финансы (финансовые цели развития и результаты работы компании — прибыль, рентабельность и т. д.).
- Клиенты и рынки (цели присутствия на рынке и показатели качества обслуживания клиентов — освоение рынков и территорий продаж, время выполнения заказа и т. д.).
- Процессы (требования к эффективности процессов — стоимость, время, количество ошибок, риски и т. д.).
- Развитие (цели поиска новых технологий и повышения квалификации персонала и т. д.).

Между всеми показателями существуют причинно-следственные влияния. Например, чем выше квалификация персонала и лучше технология ведения бизнеса, тем проще поддерживать бизнес-процессы, что, в свою очередь, способствует более качественному обслуживанию клиентов и реализации конкурентных преимуществ, а, следовательно, помогает достичь запланированных финансовых показателей. Таким образом, для компании в целом финансовые показатели — это конечная цель функционирования, тогда как прочие перспективы определяют будущий потенциал компании.

Подобным образом можно определить ключевые показатели функционирования службы информационной безопасности компании и задать перспективы развития корпоративных систем защиты информации. При этом следует помнить, поскольку технологии безопасности оказывают косвенное воздействие на финансовые показатели компании, их надо рассматривать с точки зрения вклада в развитие бизнеса. На уровне клиентской перспективы оценка технологий безопасности отражает эффективность взаимодействия соответствующего подразделения с основным бизнесом компании. Стратегия развития технологий безопасности на базе методов ССП формулируется в виде взаимосвязанного набора целей и показателей, сгруппированных по следующим перспективам:

- миссия (основное предназначение и пути развития ИТ в компании);
- клиенты (цели поддержки основной деятельности компании);
- процессы (показатели эффективности процедур разработки и внедрения);
- технологии (оценка обоснованности и эффективности используемых технологий);
- организация (показатели эффективности внутренних процедур ИТ-подразделения).

Эти перспективы могут быть отправной точкой в разработке стратегических карт, но в соответствии с ситуацией и видением руководства состав перспектив может меняться. Обязательным условием вносимых изменений является сохранение логики взаимного влияния перспектив друг на друга. Как показывает практика, при освоении идеи ССП формирование стратегических карт не представляет особых затруднений. Но, несмотря на кажущуюся простоту, менеджеры часто допускают ошибки при использовании методологии. Первая типичная ошибка заключается в создании большого набора метрик, отражающих отдельные аспекты деятельности службы безопасности, но никак не связанных друг с другом или со стратегией развития компании в целом. Вторая ошибка — формирование стратегических карт, содержащих большое число причинно-следственных взаимосвязей между целями и показателями. Оба эти варианта приводят к невозможности расстановки приоритетов в развитии корпоративной

Таблица 1

Перспективы и цели при планировании технологий безопасности

Перспектива ССП	Стратегические цели в безопасности
Финансы	1. Понимание места расходов на технологии безопасности в общей структуре бизнеса. 2. Способность контролировать затраты на безопасность. 3. Сокращение затрат на защиту информации. 4. Обеспечение возврата инвестиций в безопасность. 5. Составление контрактов на внутренние сервисы безопасности
Клиенты	1. Обеспечение доступности сервисов безопасности. 2. Измерение производительности сервисов безопасности. 3. Установление стоимостных характеристик для определенного количества и качества оказанных сервисов безопасности. 4. Обеспечение надежности АС в защищенном исполнении. 5. Поддержка обращений пользователей
Внутренние процессы	1. Сервисно-ориентированная культура предоставления сервисов безопасности. 2. Квалифицированный персонал. 3. Эффективность предоставления сервисов безопасности. 4. Время предоставления сервисов безопасности. 5. Производительность инфраструктуры предоставления сервисов безопасности. 6. Возможность учета количества предоставленных сервисов безопасности
Обучение и развитие	1. Обеспечение гибкости системы безопасности. 2. Возможность контролировать изменения в системе безопасности. 3. Обеспечение адаптации системы безопасности к изменяющимся требованиям бизнеса. 4. Формирование и передача основанных на опыте корпоративных знаний в области предоставления сервисов безопасности. 5. Способность использовать новые технологии безопасности

системы защиты информации, хотя именно методология системы сбалансированных показателей позволяет обеспечить четкое соответствие стратегии развития ИТ целям компании на формальном уровне. Пример соответствия стандартных перспектив ССП набору стратегических целей службы безопасности приведен в табл. 1.

Как и любой инструмент стратегического планирования, система сбалансированных показателей имеет возможности и ограничения в практическом применении. Использование ССП позволяет:

- устранить разрыв между разработкой стратегии безопасности и ее реализацией;

- оперативно реагировать на изменения окружающей среды;
- оценить существующую стратегию безопасности.

Однако применение методики ССП не предполагает создания стратегии развития предприятия и не требует отказа от традиционных инструментов планирования и контроля.

Совокупная стоимость владения — Total Cost of Ownership (TCO)

Совокупная стоимость владения (Total Cost of Ownership) первоначально разрабатывалась как средство расчета стоимости владения компьютером. Но в последнее время благодаря усилиям компании Gartner Group эта методика стала основным инструментом подсчета совокупной стоимости владения корпоративных систем защиты информации. Основной целью расчета TCO является выявление избыточных статей расхода и оценка возможности возврата инвестиций, вложенных в технологии безопасности. Таким образом, полученные данные по совокупной стоимости владения используются для выявления расходной части использования корпоративной системы защиты информации.

Главной проблемой при определении TCO является проблема выявления составляющих совокупной стоимости владения и их количественная оценка. Все составляющие TCO условно разделяются на «видимые» пользователю (первоначальные затраты) и «невидимые» (затраты эксплуатации и использованию). При этом «видимая» часть TCO составляет 32 %, а по некоторым оценкам и 21 %, а «невидимая» — 68 % или соответственно 79 %.

К группе «видимых» затрат относятся следующие:

- стоимость лицензии;
- стоимость внедрения;
- стоимость обновления;
- стоимость сопровождения.

Все эти затраты, за исключением внедрения, имеют фиксированную стоимость и могут быть определены еще до принятия решения о внедрении корпоративной системы защиты информации. Следует отметить, что и в «видимом» секторе поставщиками систем безопасности иногда могут использоваться скрытые механизмы увеличения стоимости для привлечения клиента.

Дополнительные затраты («невидимые») появляются у каждого предприятия, завершившего у себя внедрение корпоративной системы защиты информации. «Невидимые» затраты также разделяются на группы:

- Затраты на оборудование, включают в себя затраты на приобретение или обновление средств защиты информации, на организацию бесперебойного питания и резервного копирования информации, на установку новых устройств безопасности и пр.
- Дополнительное программное обеспечение (системы управления безопасностью, VPN, межсетевые экраны, антивирусы и пр.).
- Персонал (например, ошибки и трудности в работе со средствами защиты, неприятие или даже саботаж новых средств защиты и т. д.).
- Стоимость возможностей — стоимость возможных альтернатив. Рассматриваются следующие варианты: приобретение или обновление корпоративной системы защиты информации и сделать это собственными силами или заказать сторонней организации.
- Другие. В этом случае оценивается степень и стоимость риска «выхода из строя» системы.

Показатель TCO корпоративной системы информационной безопасности рассчитывается как сумма всех затрат, «видимых» и «невидимых». Затем этот показатель сравнивается с рекомендуемыми величинами для данного типа предприятия. Существует 17 типов предприятий, которые в свою очередь делятся на малые, средние и крупные.

Если полученная совокупная стоимость владения системы безопасности значительно превышает рекомендованное значение и приближается к предельному, то необходимо принять меры по снижению TCO. Сокращения совокупной стоимости владения можно достичь следующими способами: максимальной централизацией управления безопасностью, уменьшением числа специализированных элементов, настройкой прикладного программного обеспечения безопасности и пр.

Функционально-стоимостной анализ — Activity Based Costing (ABC)

Функционально-стоимостной анализ (ФСА) — это процесс распределения затрат с использованием первичных носителей стоимости, ориентированных на производственную и/или логистическую структуру предприятия с конечным распределением затрат по основным носителям (продуктам и услугам). Данный подход позволяет весьма точно и понятно установить связь между элементами себестоимости продукции и производственными процессами.

Применимо к оценке эффективности корпоративных систем защиты информации, метод ФСА используется для построения моделей бизнес-процессов предприятия, «Как есть» и «Как будет». Модель «Как будет»

отражает изменение технологии реализации основных бизнес-процессов при использовании выбранной корпоративной системы информационной безопасности. На основе показателей стоимости, трудоемкости и производительности определяется наилучшая модель бизнес-процессов «Как будет».

Таким образом, метод ФСА является альтернативой традиционным финансовым подходам и позволяет:

- предоставить информацию в форме, понятной для персонала предприятия, непосредственно участвующего в бизнес-процессе;
- распределить накладные расходы в соответствии с детальным просчетом использования ресурсов, подробным представлением о процессах и функциях их составляющих, а также их влиянием на себестоимость.

Следует отметить, что развитием метода ФСА стал метод функционально-стоимостного управления (ФСУ, Activity Based Management, ABM). Совместно методы ФСА и ФСУ используются для реорганизации бизнес-процессов с целью повышения производительности, снижения стоимости и улучшения качества.

Основные положения методики Total Cost of Ownership

Анализ методов оценки эффективности инвестиций в корпоративные системы информационной безопасности показывает что, только метод совокупной стоимости владения (ТСО) в явном виде позволяет рассчитать расходную часть на систему безопасности. Поэтому давайте рассмотрим методику ТСО более подробно.

Информационная безопасность обеспечивается комплексом мер на всех этапах жизненного цикла информационной системы, совокупная стоимость владения (показатель ТСО) для системы информационной безопасности 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 средства аутентификации, авторизации и администрирования (AAA).
- Затрат на обеспечение физической безопасности.
- Обучения персонала.

- Управления и поддержки системы (администрирование безопасности).
- Аудита информационной безопасности.
- Периодической модернизации системы информационной безопасности.

Таким образом, методика совокупной стоимости владения компании Gartner Group позволяет:

- получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;
- сравнить подразделения службы информационной безопасности компании, как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;
- оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ТСО.

Здесь под показателем ТСО понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. ТСО 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 комплексных информационных систем (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, аутсорсинг 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 систему информационной безопасности.

Существенно, что ТСО не только отражает «стоимость владения» отдельных элементов и связей корпоративной системы защиты информации

в течение их жизненного цикла. «Овладение методикой» TCO 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 TCO 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 TCO 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».

Известно, что в методике TCO в качестве базы для сравнения используются данные и показатели TCO 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 (Cost Profiles) с учетом данных по количеству и типам серверов, персональных компьютеров, периферии и сетевого оборудования;
- по заработанной плате сотрудников (Salary and Asset Scalars) с учетом дохода компании, географического положения, типа производства и размещения организации в крупном городе или нет;
- по конечным пользователям ИТ (End User Scalars) 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 в области управления ИБ (Best Practices) с учетом реального состояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами;

- по уровню сложности организации (Complexity Level) с учетом состояния организации конечных пользователей (процент влияния — 40 %), технологии SW (40 %), технологии HW (20 %).

В целом определение затрат компании на ИБ подразумевает решение следующих трех задач:

- оценку текущего уровня TCO корпоративной системы защиты информации и КИС в целом;
- аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня TCO;
- формирование целевой модели TCO.

Рассмотрим каждую из перечисленных задач.

1. Оценка текущего уровня TCO

В ходе работ по оценке TCO проводится сбор информации и расчет показателей TCO организации по следующим направлениям:

- существующие компоненты ИС (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.

2. Аудит информационной безопасности компании

По результатам собеседования с топ-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов:

- политики безопасности;
- организации защиты;
- 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 ТСО, 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 ТСО проверяемой компании с модельным значением показателя ТСО 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.

3. Формирование целевой модели ТСО

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 (ROSI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Виды затрат на систему информационной безопасности

Затраты на информационную безопасность подразделяются на следующие категории:

1. Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты).

1.1. Затраты на приобретение и ввод в эксплуатацию программно-технических средств: серверов, компьютеров конечных пользователей (настольные и мобильные), периферийных устройств и сетевых компонентов.

1.2. Затраты приобретение и настройку средств защиты информации.

1.3. Затраты на содержание персонала, стоимость работ и аутсорсинг.

1.4. Затраты на формирование политики безопасности предприятия.

2. Затраты на контроль (определение и подтверждение достигнутого уровня защищенности ресурсов предприятия).

2.1. 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).

2.2. Внеплановые проверки и испытания:

- оплата работы испытательного персонала специализированных организаций;
- обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами.

2.3. Контроль за соблюдением политики информационной безопасности:

- затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны;
- затраты на организацию временного взаимодействия и координации между подразделениями для решения конкретных повседневных 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.

2.4. Затраты на внешний аудит:

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

3. Внутренние затраты на ликвидацию последствий нарушений политики информационной безопасности (затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут).

3.1. 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.

3.2. Затраты на ликвидацию последствий нарушения режима информационной безопасности:

- 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.

3.3. 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.

3.4. 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, предметов посягательства, выявление мотивов неправомерных действий и т. д.);
- затраты на обновление планов обеспечения непрерывности деятельности службы безопасности.

3.5. Затраты на переделки:

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

4. Внешние затраты на ликвидацию последствий нарушения политики информационной безопасности.

4.1. 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.

4.2. 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.

4.3. 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.

5. Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (предупредительные мероприятия).

5.1. Затраты на 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.

5.2. 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 ведения архива данных;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, вычислительной техники и т. п.

5.3. Аудит системы безопасности:

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

5.4. Обеспечение должного качества информационных технологий:

- затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных нега-

тивных аспектов информационных технологий, которые влияют на целостность и доступность информации;

- затраты на доставку (обмен) конфиденциальной информации;
- удовлетворение субъективных требований пользователей: стиль, удобство интерфейса и др.

5.5. Обеспечение требований стандартов:

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

5.6. Обучение персонала:

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

Пример использования методики Total Cost of Ownership

Пусть объектом исследования является страховая компания ЗАО «Страхование». Название компании вымышленное, возможные совпадения случайны и носят не преднамеренный характер.

Для определения затрат на систему информационной безопасности по методике совокупной стоимости владения воспользуемся программным продуктом «TCO Manager» компании Gartner Group. Технология работы с ПП «TCO Manager» заключается в следующем: пользователь вводит первоначальные данные об объекте (профайл компании, данные о конечных пользователях, об информационных активах предприятия), исходя из них определяется текущий показатель TCO и вычисляются ежегодные затраты на поддержание существующей уровня безопасности. Также «TCO Manager» позволяет оптимизировать показатель TCO, сравнив текущий показатель TCO компании с «лучшим» в отрасли и смоделировав целевой показатель TCO для данного предприятия.

Теперь обратимся к исходным данным по ЗАО «Страхование» и вычислим текущий показатель TCO:

- Название компании — **ЗАО «Страхование».**
- Период анализа — **январь–декабрь 2004.**
- Основной вид деятельности — **страхование.**
- Общий годовой доход — **450 млн руб.**

Таблица 2

Классификация конечных пользователей по типам

Тип конечных пользователей	В процентном отношении, %	Количество, чел.
Руководящий персонал	1	29
Научные работники	20	574
Исполнительный персонал	75	2152
Операторы	4	115
Общее количество	100	2869

- Количество рабочих часов в год — **1 880 час/год.**
- Средняя годовая зарплата конечных пользователей **38 000 руб.**
- Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д., персонала службы безопасности (ECH) — **37 %.**
- Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д., конечных пользователей (ECH) — **37 %.**
- Количество конечных пользователей — **2 869 чел.**

Классификация конечных пользователей представлена в табл. 2, 3.

Форма ввода данных «Интервью» в «TCO Manager» содержит сведения об информационных активах предприятия (аппаратные средства и программное обеспечение), информацию о конечных пользователях, и на основании этих данных мы получаем следующие отчеты (табл. 4–6).

Таблица 3

Классификация конечных пользователей по местоположению

Тип местоположения	В процентном отношении, %	Количество, чел.
Desktop	85	2439
Mobile	10	287
Telecommuters	5	143
Общее количество	100	2869

Таблица 4

Текущие затраты на сетевое оборудование

Сетевое оборудование	Текущие затраты, тыс. руб.
Servers	90
Client — Desktop	2810
Client — Mobile	350
Peripherals	617
Network Device Assets	212
Total Assets	4079

Также «TCO Manager», используя практический подход к определению совокупной стоимости владения, позволяет сравнивать текущие затраты с эталонными («лучшими в группе») и строить целевые показатели затрат (см. табл. 6–16). В частности, в табл. 7–16 приведена детализация и расшифровка укрупненных прямых и косвенных затрат, которые отображены в табл. 6.

Целевые показатели являются моделируемыми на основании проекта модернизации корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации (физическая защита).

Условно определяют три возможных состояния системы защиты КИС от вирусов и вредоносного программного обеспечения, а именно: базовое, среднее и высокое. Рассмотрим характеристики этих состояний:

- **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 враждебного программного обеспечения 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 сети Интернет. Дополнительно к техническим мерам активно предлагаются и используются организационные меры защиты информации.

Таблица 5

Сравнение текущего и целевого состояния системы защиты

Критерии	Текущий уровень	Целевой уровень
Усовершенствование технологии управления активами		
Автоматизированное управление активами	Базовый	Высокий
Учет программного обеспечения	Базовый	Высокий
Учет аппаратных средств	Базовый	Высокий
Усовершенствование технологии управления системы		
Системы обнаружения вирусов и защиты	Базовый	Высокий
Системное управление	Базовый	Средний
Стандартизация процессов модернизации		
Стандартизация поставщиков	Базовый	Средний
Стандартизация платформы	Средний	Высокий
Совершенствование управления персоналом		
Обучение пользователей	Базовый	Высокий
Обучение ИТ-специалистов	Базовый	Средний
Мотивация ИТ-персонала	Базовый	Средний
Организация устойчивой ИТ-службы	Базовый	Средний

- **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.

Согласно практическому подходу (best practice) в «TCO Manager» формируется отчет (табл. 5) для ЗАО «Страхование», в котором отражаются требования к состоянию корпоративной системы защиты на основании данных о типе предприятия и текущего показателя TCO.

Таким образом, можно сделать вывод о том, что ЗАО «Страхование» необходимо повышать уровень защиты информационной системы от вирусов, совершенствовать технологию управления активами и проводить обучение конечных пользователей и специалистов отдела информационных технологий.

Таблица 6

Анализ затрат по показателям TCO

Категории затрат	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Прямые затраты									
Затраты на программное обеспечение и оборудование	5 601 557	4 931 610	5 400 695	–669 947	–12	469 085	10	200 862	–4
Операционные затраты (управление)	4 831 911	4 711 401	2 695 527	–120 511	–2	–2 015 873	–43	–2 136 384	–44
Административные затраты (поддержка)	1 477 957	994 636	1 272 225	–483 321	–33	277 589	28	–205 732	–14
Общие прямые	**11 911 426**	**10 637 647**	**9 368 447**	**–1 273 779**	**–11**	**–1 269 199**	**–12**	**–2 542 978**	**–21**
Косвенные затраты									
Поддержка конечных пользователей	11 853 266	20 458 366	9 005 139	8 605 100	73	–11 453 227	–56	–2 848 127	–24
Простой	2 619 053	636 117	1 491 347	–1 982 936	–76	855 230	134	–1 127 705	–43
Общие косвенные	**14 472 318**	**21 094 483**	**10 496 486**	**6 622 165**	**46**	**–10 597 997**	**–50**	**–3 975 832**	**–27**
Ежегодный TCO	26 383 744	31 732 130	19 864 933	5 348 386	20	–11 867 196	–37	–6 518 811	–25
Процент TCO от дохода	59	71	44	12	203	–26	–374	–14	–247
Процент прямых затрат от дохода	26	24	21	–03	–107	–03	–119	–06	–213

Таблица 7

Детализация затрат на программное обеспечение и оборудование по категориям

Категории затрат на программное обеспечение и оборудование	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Оборудование	2 451 546	2 617 140	2 836 522	165 594	7	219 382	8	384 976	16
Программное обеспечение	2 873 154	2 040 780	2 262 723	–832 374	–29	221 943	11	–610 431	–21
Оборудование ИС	79 617	78 690	89 665	–927	–1	10 975	14	10 048	13
Программное обеспечение ИС	197 240	195 000	211 786	–2 240	–1	16 786	9	14 546	7
Общие затраты	**5 601 557**	**4 931 610**	**5 400 695**	**–669 947**	**–12**	**469 085**	**10**	**–200 862**	**–4**

Таблица 8

Расшифровка затрат на аппаратные средства

Категории затрат на аппаратные средства	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Покупка оборудования	1 909 668	1 894 950	2 109 357	–14 718	–1	214 407	11	199 689	10
Лизинговые платежи	307 521	260 480	395 994	–47 041	–15	135 514	52	88 473	29
Модернизация	67 972	258 340	57 254	190 368	280	–201 086	–78	–10 717	–16
Комплектующие	81 855	36 640	165 148	–45 215	–55	128 508	351	83 292	102
Лицензии	84 530	166 730	108 769	82 200	97	–57 961	–35	24 238	29
Общие затраты	**2 451 546**	**2 617 140**	**2 836 522**	**165 594**	**7**	**219 382**	**8**	**384 976**	**16**

Таблица 9

Расшифровка затрат на программное обеспечение

Категории затрат на программное обеспечение	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на собственную разработку программных продуктов и баз данных	502 767	352 500	427 128	–150 267	–30	74 628	21	–75 639	–15
Затраты на бизнес-приложения и инженерное программное обеспечение	1 179 383	1 393 000	1 002 000	213 617	18	–391 000	–28	–177 382	–15
Затраты на средства и инструменты разработки	410 817	57 480	357 167	–353 337	–89	299 687	521	–53 650	–13
Затраты на формирование системы внутренних коммуникаций	163 804	49 400	142 425	–114 404	–70	93 025	188	–21 379	–13
Другие	616 384	188 400	334 003	–427 984	–69	145 603	77	–282 381	–46
Общие затраты	**2 873 154**	**2 040 780**	**2 262 723**	**–832 374**	**–29**	**221 943**	**11**	**–610 431**	**–21**

Таблица 10

Детализация операционных затрат

Операционные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Операционные затраты									
Обслуживание клиентских мест и периферийных устройств	1 563 387	2 473 600	836 474	910 213	58	–1 637 126	–66	–726 913	–46
Обслуживание серверов	559 468	427 961	336 049	–131 507	–24	–91 912	–21	–223 419	–40
Обслуживание сети	223 624	253 680	171 567	30 056	13	–82 113	–32	–52 056	–23
Планирование и управление процессами	460 701	0	329 119	–460 701	–100	329 119	Undefined	–131 582	–29
Обслуживание и администрирование баз данных	241 331	0	230 757	–241 331	–100	230 757	Undefined	–10 574	–4
Затраты на сервисную поддержку	1 783 400	1 556 160	791 561	–227 240	–13	–764 599	–49	–991 839	–56
Общие ежегодные затраты	**4 831 911**	**4 711 401**	**2 695 527**	**–120 511**	**–2**	**–2 015 873**	**–43**	**–2 136 384**	**–44**

Таблица 11

Расшифровка затрат на обслуживание клиентских мест и периферийных устройств

Затраты на обслуживание клиентских мест и периферийных устройств	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2 уровня	247 995	494 720	121 749	246 725	99	–372 971	–75	–126 246	–51
Решение проблем 3 уровня	86 580	296 832	32 519	210 252	243	–264 313	–89	–54 061	–62
Планирование и управление трафиком	32 449	123 680	30 753	91 231	281	–92 927	–75	–1 696	–5
Точная настройка	24 337	74 208	22 871	49 871	205	–51 337	–69	–1 466	–6
Администрирование конечных пользователей	62 903	296 832	33 507	233 929	372	–263 325	–89	–29 396	–47
Поддержка операционной системы	50 821	74 208	23 106	23 387	46	–51 102	–69	–27 715	–55
Обслуживание рабочей силы	105 663	123 680	72 396	18 017	17	–51 284	–41	–33 267	–31
Установка программного обеспечения	387 563	321 568	268 821	–65 995	–17	–52 747	–16	–118 742	–31
Управление приложениями	225 460	74 208	74 208	–151 252	–67	18 037	24	–133 215	–59
Конфигурация аппаратных средств	49 525	197 888	24 539	148 363	300	–173 349	–88	–24 985	–50
Установка аппаратных средств	120 721	123 680	41 130	2 959	2	–82 550	–67	–79 591	–66
Управление дисками и файлами	29 736	74 208	14 963	44 472	150	–59 245	–80	–14 773	–50
Планирование вместимостью архива	8 980	49 472	7 252	40 492	451	–42 220	–85	–1 729	–19
Резервное копирование и архивирование	130 654	123 680	50 622	–6 974	–5	–73 058	–59	–80 032	–61
Управление архивами	0	24 736	0	24 736	Undefined	–24 736	–100	0	–
Общие ежегодные затраты	**1 563 387**	**2 473 600**	**836 474**	**910 213**	**58**	**–1 637 126**	**–66**	**–726 913**	**–46**

Таблица 12

Расшифровка затрат на обслуживание серверов

Затраты на обслуживание серверов	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2 уровня	73 882	85 592	29 237	11 711	16	–56 356	–66	–44 645	–60
Решение проблем 3 уровня	43 166	51 355	23 722	8 189	19	–27 633	–54	–19 444	–45
Планирование и управление трафиком	18 721	21 398	9 812	2 677	14	–11 586	–54	–8 908	–48
Точная настройка	18 721	12 839	9 730	–5 882	–31	–3 109	–24	–8 991	–48
Администрирование конечных пользователей	22 642	51 355	14 304	28 714	127	–37 051	–72	–8 337	–37
Поддержка операционной системы	21 481	12 839	13 687	–8 642	–40	848	7	–7 794	–36
Обслуживание рабочей силы	17 026	21 398	10 481	4 372	26	–10 917	–51	–6 544	–38
Установка программного обеспечения	46 023	55 635	24 230	9 612	21	–31 404	–56	–21 792	–47
Управление приложениями	28 751	12 839	12 434	–15 912	–55	–405	–3	–16 317	–57
Конфигурация аппаратных средств	143 021	34 237	94 451	–108 784	–76	60 215	176	–48 569	–34
Установка аппаратных средств	44 956	21 398	31 956	–23 558	–52	10 558	49	–13 000	–29
Управление дисками и файлами	27 732	12 839	16 619	–14 894	–54	3 780	29	–11 114	–40
Планирование вместимостью архива	5 783	8 559	4 175	2 777	48	–4 384	–51	–1 607	–28
Резервное копирование и архивирование	24 229	21 398	20 786	–2 831	–12	–612	–3	–3 444	–14
Управление архивами	23 335	4 280	20 423	–19 056	–82	16 143	377	–2 913	–12
Общие ежегодные затраты	**559 468**	**427 961**	**336 049**	**–131 507**	**–24**	**–91 912**	**–21**	**–223 419**	**–40**

Таблица 13

Расшифровка затрат на планирование и управление процессами

Затраты на планирование и управление процессами	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Управление стоимостью	69 097	0	67 866	–69 097	–100	67 866	Undefined	–1 232	–2
Управление системными исследованиями планированием и продуктами	117 328	0	69 918	–117 328	–100	69 918	Undefined	–47 410	–40
Оценка закупок	86 071	0	76 853	–86 071	–100	76 853	Undefined	–9 218	–11
Безопасность и защита от вирусов	169 951	0	103 863	–169 951	–100	103 863	Undefined	–66 088	–39
Затраты на восстановление бизнеса	18 254	0	10 620	–18 254	–100	10 620	Undefined	–7 634	–42
Общие ежегодные	**460 701**	**0**	**329 119**	**–460 701**	**–100**	**329 119**	**Undefined**	**–131 582**	**–29**

Таблица 14

Детализация административных затрат

Административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Финансовые и административные затраты	795 837	665 036	575 326	–130 801	–16	–89 710	–13	–220 511	–28
Затраты на обучение ИТ-специалистов	188 798	114 240	188 339	–74 558	–39	74 099	65	–459	0
Обучение конечных пользователей	493 322	215 360	508 560	–277 962	–56	293 200	136	15 237	3
Общие ежегодные	**1 477 957**	**994 636**	**1 272 225**	**–483 321**	**–33**	**277 589**	**28**	**–205 732**	**–14**

Таблица 15

Расшифровка финансовых и административных затрат

Финансовые и административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на контроль	388 410	199 511	317 198	–188 899	–49	117 688	59	–71 211	–18
Административная помощь сотрудникам ИТ отдела	39 656	133 007	36 556	93 351	235	–96 451	–73	–3 101	–8
Управление активами	70 323	66 504	17 374	–3 819	–5	–49 129	–74	–52 949	–75
Бюджетирование	36 128	66 504	32 001	30 375	84	–34 502	–52	–4 127	–11
Аудит	18 032	33 252	10 023	15 220	84	–23 229	–70	–8 009	–44
Управление приобретением и контрактованием	84 239	133 007	54 290	48 768	58	–78 717	–59	–29 949	–36
Управление вендорами	159 048	33 252	107 883	–125 797	–79	74 632	224	–51 165	–32
Общие ежегодные	**795 837**	**665 036**	**575 326**	**–130 801**	**–16**	**–89 710**	**–13**	**–220 511**	**–28**

Таблица 16

Расшифровка затрат на поддержку конечных пользователей

Затраты на поддержку конечных пользователей	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на поддержку	5 421 467	6 507 639	3 799 406	1 086 172	20	–2 708 233	–42	–1 622 061	–30
Затраты на самостоятельное изучение и поддержку	4 265 978	4 743 988	3 149 395	478 010	11	–1 594 593	–34	–1 116 583	–26
Формальное обучение	1 171 363	960 321	1 086 988	–211 041	–18	126 667	13	–84 375	–7
Управление данными	535 383	1 258 021	508 870	722 639	135	–749 151	–60	–26 512	–5
Разработка приложений	459 075	691 431	460 479	232 357	51	–230 953	–33	1 404	0
Форс-мажор	0	6 296 965	0	6 296 965	Undefined	–6 296 965	–100	0	–
Общие ежегодные	**11 853 266**	**20 458 366**	**9 005 139**	**8 605 100**	**73**	**–11 453 227**	**–56**	**–2 848 127**	**–24**

Теперь обратимся к отчетам по совокупной стоимости владения, приведенным в таблицах, и проанализируем полученные показатели TCO.

Сопоставляя результаты сравнения в табл. 5 и данные отчетов (табл. 6–16), можно сделать следующие выводы: при построении целевой модели TCO наибольшему снижению подверглись административные затраты на управление (на 44 %) и затраты при простое (на 43 %). Сокращение административных расходов связано, в основном, с внедрением автоматизированной системы управления активами, а значительное снижение затрат от простоев — с пересмотром уровня знаний конечных пользователей и ИТ-персонала и увеличением затрат на обучение.

Небольшое повышение затрат на аппаратные средства (на 16 %) вызвано закупкой оборудования, необходимого для внедрения корпоративной системы защиты.

Таким образом, целевой показатель TCO значительно меньше текущего, но вместе с тем поддержание соответствующего уровня защиты требует существенных расходов (5–7 % от ежегодного дохода) и для обоснования этих расходов необходимо применять методы оценки эффективности инвестиций в корпоративную систему информационной безопасности.

Литература

1. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. 416 с.
2. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. ; М.: ДМК Пресс, 2004. 400 с.
3. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.