МЕТОДИКА ЭКСПЕРТНО-АНАЛИТИЧЕСКОГО АНАЛИЗА ТЕХНИКО ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ СРАВНЕНИЯ С «ЛУЧШИМИ ПРАКТИКАМИ»

Гайдамакин Н. А.[1]

DOI: 10.21681/2311-3456-2025-5-149-161

Цель статьи: *рассмотреть методы анализа эффективности систем обеспечения информационной безопасности предприятий и сформировать методику экспертно-аналитического анализа их технико-экономической эффективности на основе сравнения «с лучшими практиками».*

Метод исследования: *применение методов анализа эффективности IT-сферы предприятий на основе принципов «совокупной стоимости владения».*

Результаты исследования: *рассмотрены и проанализированы проблемы двух основных подходов к анализу эффективности систем обеспечения информационной безопасности предприятий – риск-ориентированного и технико-экономического.*

На основе анализа технико-экономической эффективности по принципу «совокупной стоимости владения» в сфере информационных технологий проведена систематизация расходов (затрат) на обеспечение информационной безопасности предприятия в виде двух-уровневой иерархической схемы – капитальные затраты (по стоимости приобретения и установки средств технической защиты информации и средств обеспечения безопасности информационных технологий, затрат на проведение организационно-технических и организационно-штатных мероприятий, амортизационные потери), эксплуатационные затраты (на заработную плату и аутсорсинг, на сопровождение и техническое обслуживание, на обучение персонала, на предупредительно-профилактические мероприятия в виде аудита, пентестинга, тренировок и учений), затраты и потери, связанные с результативно-целевой стороной системы обеспечения информационной безопасности (потери от простоя корпоративной информационной системы в результате компьютерных инцидентов, затраты на ее восстановление, потери рабочего времени на организационно-технологические процедуры защиты информации в виде времени прохождения процедур идентификации и аутентификации, блокирования автоматизированных рабочих мест в результате неправильных действий пользователей).

Представлена целевая функция технико-экономической эффективности системы обеспечения информационной безопасности на основе взвешенного суммирования показателей эффективности по составляющим представленной схемы затрат, сравниваемых с «лучшими практиками» или среднестатистическими значениями по отрасли предприятия.

Сформирована методика анализа технико-экономической эффективности систем обеспечения информационной безопасности предприятий на основе представленной целевой функции и применения метода экспертных оценок для учета специфики предприятий по особенностям IT-инфраструктуры, бизнес-политики и политики информационной безопасности. По сформированной методике приведен иллюстративный пример результатов анализа технико-экономической эффективности системы обеспечения информационной безопасности предприятия.

Научная новизна: *проведена систематизация расходов, затрат и потерь на обеспечение информационной безопасности в методологии «совокупной стоимости владения», предложена суперпозиционная целевая функция и основанная на ней экспертно-аналитическая методика анализа технико-экономической эффективности систем обеспечения информационной безопасности.*

Ключевые слова: *система обеспечения информационной безопасности, эффективность, совокупная стоимость владения, риск-ориентированной анализ, технико-экономический анализ, экспертно-аналитический анализ, затраты на обеспечение информационной безопасности.*

1 Гайдамакин Николай Александрович, доктор технических наук, профессор, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия, E-mail: n.a.gaidamakin@urfu.ru

Введение

Система обеспечения информационной безопасности (СОИБ) является неотъемлемым элементом организационно-технологической инфраструктуры любого современного предприятия и по обобщенному представлению на основе национальных стандартов 27-й серии[2], требований регуляторов[3] и других нормативно-методических документов[4] включает совокупность сил и средств, мероприятий (процессов) и локальной нормативной базы.

Соответственно в бюджет любого предприятия входит раздел расходов на создание и функционирование СОИБ и для собственника (руководства) предприятия возникает необходимость анализа (оценки) эффективности соответствующих расходов.

Под эффективностью в общем смысле понимается достижение каких-либо определенных результатов с минимальными возможными издержками, приближение к максимальному (наиболее желательному) результату при минимальных негативных последствиях и возможных издержках. Во многих случаях понятие «эффективность» связано с понятием «качество» и широко используется в сфере управления (менеджмента) качеством, которая регламентируется международными стандартами серии 9000. В ГОСТ Р ИСО 9000[5] приводится следующее «классическое» определение понятия «эффективность» – соотношение между достигнутым результатом и использованными ресурсами.

Данное определение применимо к самым разнообразным сферам деятельности. Но при этом главными проблемами являются определение понятия «результат» в соответствующей сфере деятельности (и соответственно его измерение, подсчёт) и понятия «использованные ресурсы».

Эти проблемы в полной мере относятся к оценке эффективности СОИБ.

Как и во многих других случаях, «результат деятельности» в сфере обеспечения ИБ выражается качественными понятиями – «обеспечение информационной безопасности», «нейтрализация угроз безопасности информации», «недопущение инцидентов», «своевременная ликвидация последствий инцидентов» и т.д.

Общепринятый подход экономической оценки эффективности, основанный на т.н. «принципе возврата инвестиций» [1, 2], требует определения получаемой прибыли от создания и функционирования СОИБ (экономический эффект от затрат на ИБ), что, как и в отношении других участков, обеспечивающих основную деятельность предприятия, является трудно формализуемой задачей.

Определенные трудности возникают также и с понятием и оценкой затрат на создание и функционирование СОИБ. Конечно, часть затрат имеет объективную учетную основу в системе финансово-экономического документирования деятельности предприятия. Однако в отношении таких затрат, расходов или потерь, связанных с целевой результативностью СОИБ, как, например, потери рабочего времени сотрудников из-за необходимости выполнения процедур ИБ (идентификации и аутентификации), блокирование доступа к их АРМ в результате неправильных действий или ошибок по процедурам ИБ и т.п., требуется введение сложной и затратной системы фиксации соответствующих ситуаций и событий, введение дополнительных показателей внутренней отчетности, что, в свою очередь, вызывает дополнительные расходы.

Очевидно, из-за сложностей с формализацией соответствующих понятий в сфере ИБ в настоящее время нет нормированного определения (в стандартах) понятия «эффективность обеспечения ИБ», «эффективность системы обеспечения информационной безопасности» и несмотря на большую совокупность работ по анализу эффективности обеспечения ИБ [3–9] отсутствуют общепринятые модели и методики оценки эффективности СОИБ.

1. Основные методы оценки эффективности систем обеспечения информационной безопасности

Можно выделить два подхода (метода) к анализу эффективности обеспечения ИБ – «угрозный» или иначе «риск-ориентированный»[6] [8–10] и «технико-экономический»[7] [11, 12].

В первом подходе в качестве результата обеспечения ИБ рассматривается снижение или нейтрализация угроз безопасности информации (снижение их вероятности, потока угроз, их интенсивности, «опасности») или производных от этих понятий, в частности, т.н. «риска» R от угроз безопасности информации. Соответственно эффективность СОИБ $Эфф_{СОИБ}$ рассматривается как соотношение

2 ГОСТ Р ИСО/МЭК 27001–2021 «Информационная технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», ГОСТ Р ИСО/МЭК 27002–2021 «Информационная технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», Проект ГОСТ Р «Защита информации. Система организации и управления защитой информации. Общие положения».

3 Методический документ «Методика оценки состояния защиты информации в органе (организации)». Утвержден ФСТЭК России 02.05.2024.

4 Стандарт Банка России СТО БР ИББС–1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

5 ГОСТ Р ИСО 9000–2015 «Системы менеджмента качества. Основные положения и словарь».

6 ГОСТ Р ИСО/МЭК 27005––2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

7 См. также: Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс. 2004. 384 с.

величины уменьшения риска ΔR от угроз безопасности к стоимости затрат:

$$Эфф_{СОИБ} = \frac{R - R_{СОИБ}}{C_{СОИБ}}, \quad (1)$$

где $R_{СОИБ}$ – «остаточный» риск от угроз безопасности информации в результате создания и функционирования СОИБ; $C_{СОИБ}$ – стоимость создания и функционирования СОИБ.

В целях нормирования показателя эффективности $Эфф_{СОИБ}$ в знаменатель соотношения (1) добавляется стоимость $C_{ИТ/СОИБ}$ всей IT-системы предприятия (IT-инфраструктуры) без учета стоимости СОИБ:

$$Эфф_{СОИБ} = \frac{R - R_{СОИБ}}{C_{ИТ/СОИБ} + C_{СОИБ}}. \quad (2)$$

При этом под «риском» R понимается математическое ожидание возможного ущерба от реализации угрозы безопасности:

$$R = P_{возн}\, C_{объект}, \quad (3)$$

где $P_{возн}$ – вероятность возникновения угрозы безопасности; $C_{объект}$ – стоимость объектов защиты, на которые воздействует угроза, точнее говоря, величина потерь от реализации воздействия угрозы безопасности на соответствующие объекты.

Вероятность возникновения какой-либо угрозы безопасности информации определяется целым рядом трудно формализуемых факторов, характеризующих источник угрозы (злоумышленника, нарушителя ИБ) и объект воздействия, среди которых в 1-ю очередь следует выделить мотивацию источника *Мотив*, его подготовленность *Подг*, оснащенность *Оснащ* и осведомленность *Освед* (о СОИБ). В результате при гипотезе о независимости действия источников угроз безопасности вероятность $P_{возн_i}$ возникновения i-й угрозы определяется следующим соотношением:

$$P_{возн_i} = 1 - \prod_{k=1}^{K_i} \left(1 - P_{ист_{ik}}(Мотив_{ik}, Подг_{ik}, Оснащ_{ik}, Освед_{ik})\right), \quad (4)$$

где $P_{ист_{ik}}(Мотив_{ik}, Подг_{ik}, Оснащ_{ik}, Освед_{ik})$ – функция (функционал) определения вероятности возникновения i-й угрозы от k-го источника, в зависимости от его мотивации $Мотив_{ik}$, подготовленности $Подг_{ik}$, оснащенности $Оснащ_{ik}$ и осведомленности $Освед_{ik}$; K_i – количество идентифицированных источников i-й угрозы.

Риск от возникновения i-й угрозы:

$$R_i = \sum_{m=1}^{M} C_{объект_m} \delta^{(угр)}_{im} \times \left(1 - \prod_{k=1}^{K_i}(1 - P_{ист_{ik}}(Мотив_{ik}, Подг_{ik}, Оснащ_{ik}, Освед_{ik})\right), \quad (5)$$

где M – количество объектов воздействия угроз безопасности (объектов защиты); $C_{объект_m}$ – стоимость m-го объекта защиты; $\delta^{(угр)}_{im}$ – индикатор воздействия i-й угрозы на m-й объект защиты $\delta^{(угр)}_{im} = 1$, если i-я угроза воздействует на m-й объект защиты, и $\delta^{(угр)}_{im} = 0$ в противном случае).

Риск от возникновения всех угроз безопасности:

$$R = \sum_{i=1}^{I}\sum_{m=1}^{M} C_{объект_m}\delta^{(угр)}_{im} \times \left(1 - \prod_{k=1}^{K_i}(1 - P_{ист_{ik}}(Мотив_{ik}, Подг_{ik}, Оснащ_{ik}, Освед_{ik})\right), \quad (6)$$

где I – количество идентифицированных угроз безопасности информации.

Остаточный риск $R_{СОИБ}$ определяется как математическое ожидание ущерба от вероятности реализации угроз безопасности с учетом функционирования СОИБ. Вероятность реализации угрозы безопасности рассматривается как произведение вероятности ее возникновения $P_{возн}$ на вероятность преодоления $P_{преод}$ ею системы защиты, т.е. СОИБ:

$$R_{СОИБ} = P_{возн}\, P_{преод}\, C_{объект}. \quad (7)$$

Вероятность $P_{преод_i}$ преодоления i-й угрозой СОИБ определяется вероятностью ее нейтрализации $P_{СЗИ}$ установленными средствами технической защиты информации (СТЗИ, СЗИ, СОБИТ[8]), которая в свою очередь определяется их техническими характеристиками *Техн*:

$$P_{преод_i} = 1 - \prod_{j=1}^{J}\left(1 - P_{СЗИ_{ij}}(Техн_{ij})\right), \quad (8)$$

где J – количество СЗИ; $Техн_{ij}$ – технические характеристики j-го СЗИ, влияющие на вероятность нейтрализации i-й угрозы; $P_{СЗИ_{ij}}$ – функция (функционал) определения вероятности нейтрализации i-й угрозы j-м СЗИ.

Остаточный риск $R_{СОИБ}$ от реализации всех идентифицированных угроз:

$$R_{СОИБ} = \sum_{i=1}^{I}\sum_{m=1}^{M} C_{объект_m}\delta^{(угр)}_{im} \times \left(1 - \prod_{j=1}^{J}\left(1 - P_{СЗИ_{ij}}(Техн_{ij})\right)\right) \times \left(1 - \prod_{k=1}^{K_i}(1 - P_{ист_{ik}}(Мотив_{ik}, Подг_{ik}, Оснащ_{ik}, Освед_{ik})\right). \quad (9)$$

8 Из анализа нормативных правовых актов основного регулятора в сфере ИБ – ФСТЭК России, следует, что СТЗИ (СЗИ) – это программно-аппаратные, программные или специальные технические средства, сертификация которых осуществляется на основе утвержденных профилей защиты или специальных требований к данному виду средств по обеспечению защиты информации, издаваемых регулятором. Средства обеспечения безопасности информационных технологий (СОБИТ) – это программно-аппаратные или программные средства, применяемые в системах обеспечения безопасности корпоративных сетей, но для которых нет профилей защиты (не разработаны) или нет специальных требований ФСТЭК России (не изданы). Сертификация СОБИТ осуществляется по требованиям доверия, установленным приказом ФСТЭК России от 02.06.2020 № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

Определение вида функций (точнее функционалов) $P_{\text{ист}_{ik}}$, $P_{\text{СЗИ}_{ij}}$, как и их аргументов (функций) *Мотив, Подг, Оснащ, Освед, Техн* представляет собой трудно формализуемую задачу, поэтому на практике используются экспертные оценки [13], различные эвристики и порядковые (качественные) шкалы оценивания, а также аппарат нечетких множеств [14–17] как в отношении самих аргументов *Мотив, Подг, Оснащ, Освед, Техн*, так величин $P_{\text{возн}}$, $P_{\text{преод}}$, $P_{\text{СЗИ}}$. В качестве примера можно привести попытку создания количественно-качественной методики оценки т.н. «потенциала» нарушителя ИБ, которая была представлена в проекте «Методики определения угроз безопасности информации в информационных системах» ФСТЭК России в 2015 г.

Отдельную и также трудно-формализуемую проблему составляет оценка стоимости объектов защиты $C_{\text{объект}_m}$, поскольку в большинстве случаев даже эвристическим образом не удается полностью идентифицировать и формализовать все факторы, влияющие (определяющие) на стоимость объектов защиты, в т.ч. с учетом потерь, например, репутационных, в результате воздействия на объект защиты угроз безопасности. В итоге опять-таки для оценивания $C_{\text{объект}_m}$ широко применяются экспертные оценки, порядковые шкалы и в т.ч. аппарат нечетких множеств.

Несмотря на указанные проблемы риск-ориентированные подходы к оценке эффективности систем защиты информации широко используются на практике и реализованы в методиках и поддерживающих их программно-инструментальных средствах ряда известных зарубежных и отечественных ИБ компаний – методики CRAMM (Великобритания), RickWatch (США), ГРИФ (Россия)[9]. В некоторых последних исследованиях вопросов современного состояния информационной безопасности предприятий[10] отмечается, что 89 % компаний проводят оценку критических рисков ИБ, но только 5% компаний ориентируются на оценку рисков при бюджетировании ИБ.

Технико-экономический подход к анализу эффективности СОИБ базируется на принципах и методике анализа эффективности сферы IT-предприятий [18, 19][11], разработанных в конце 80-х – середине 90-х годов известной исследовательской консалтинговой компанией Gartner Group, и включает определение и анализ двух ключевых параметров по СОИБ – совокупной стоимости владения (*TCO* – total cost of ownership) и возврата инвестиций (*ROI* – return of investment).

Наиболее показательным в смысле экономической эффективности является параметр *ROI*, определяемый как отношение суммы прибыли или убытков к сумме инвестиций (затрат). Вместе с тем, как уже отмечалось, вычленить степень непосредственного влияния функционирования СОИБ на прибыль предприятия в структуре инвестиций среди других «обеспечивающих» направлений деятельности (внедрение новых технологий и оборудования, организационно-технологические изменения и т.д.) практически невозможно.

Подход *TCO* включает анализ первоначальных и эксплуатационных, прямых и косвенных расходов на СОИБ ($TCO_{\text{СОИБ}}$) обычно в процентах по отношению к *TCO* всего предприятия ($TCO_{\text{Предпр}}$). Такой подход, прежде всего, обеспечивает понимание (представление) относительной величины и картины расходов на ИБ предприятия. При этом с учетом того, что затраты на ИБ предприятия в целом рассматриваются как необходимые (неизбежные) издержки (потери) бизнеса, то в качестве критерия эффективности СОИБ принимается снижение (минимизация) этих издержек или сравнение с т.н. «лучшими практиками» (best practices), т.е. со средними $TCO_{\text{СОИБ}}$ предприятий такой же сферы, такого же масштаба. По критерию сравнения с «лучшими практиками, чем ближе $TCO_{\text{СОИБ}}$ предприятия к средним показателям $TCO_{\text{СОИБ}}$ по отрасли, тем больше эффективность СОИБ.

Практическое применение методик анализа эффективности СОИБ на основе *TCO* включает, прежде всего, определение структуры расходов и создание системы их фиксации в финансово-производственной отчетности и документации предприятия (организации).

2. Обобщенная структура затрат на систему обеспечения информационной безопасности

В известной работе Петренко С. А. и Симонова С. В. «Управление информационными рисками. Экономически оправданная безопасность»[12] выделена следующая структура т.н. «систематических» затрат на функционирование СОИБ (после того, как она создана), состоящая из 3-х групп – затраты на обслуживание СОИБ (управление СОИБ, регламентное обслуживание СЗИ, аудит, обучение персонала и т.д.), затраты на контрольные мероприятия (плановые и внеплановые испытания и проверки, пересмотр политики безопасности и моделей угроз, контрольные мероприятия внешних структур, обусловленные регламентацией и надзорной деятельностью регуляторов и т.д.), затраты на ликвидацию

9 См.: Современные методы и средства анализа и контроля рисков информационных систем компаний. [Электронный ресурс]. URL: https://www.ixbt.com/cm/informationsystem-risks012004.shtml (Дата обращения 12.08.25).

10 Инвестиции в информационную безопасность России. Июнь 2025 г. [Электронный ресурс]. URL: https://www.csr.ru/upload/iblock/448/yzkej5xg955rh52v2eyakztjekt0rqc7.pdf (Дата обращения 12.08.25).

11 См. также: Аншина М. Л. Оценка эффективности ИТ // Системы управления бизнес-процессами". [Электронный ресурс]. URL: https://journal.itmane.ru/node/591?ysclid=me29t5rk6t214544958 (Дата обращения 12.08.25).

12 Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи, ДМК Пресс. 2004. 384 с.

последствий нарушения ИБ (восстановление IT-инфраструктуры и СОИБ, их элементов в результате инцидентов ИБ, ликвидация последствий инцидентов ИБ).

Обобщая подходы к категориям и перечням затрат на ИБ, отталкиваясь в т.ч. от методики расчета TCO в IT-сфере компании Gartner Group и учитывая современные подходы к анализу экономической эффективности IT-сферы [18, 19], можно сформировать следующую систему затрат на СОИБ, определяющих $TCO_{\text{СОИБ}}$.

1. ***Капитальные затраты*** (первоначальные и текущие) на создание и развитие СОИБ – $TCO_{\text{СОИБ}}^{(\text{Кап})}$, включая:
   - затраты (первоначальные и текущие) на приобретение и установку СТЗИ-СОБИТ – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}}}$;
   - затраты (первоначальные и текущие) по организационно-техническим и организационно-штатным мероприятиям на создание и развитие СОИБ (на получение лицензий/разрешений, аттестацию по требования ИБ корпоративной информационной системы и/или ее элементов (ИС, АС. АСУТП), на создание ИБ-подразделений и/или штатных должностей по ИБ в других подразделениях, на возможный реинжиниринг бизнес-процессов в связи с созданием или модернизацией СОИБ) – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Оргтех}}}$;
   - амортизационные потери по СОИБ (за счет амортизации стоимости СТЗИ-СОБИТ, устаревания и/или потери перспективности тех или иных видов приобретенных СТЗИ-СОБИТ и технологий, снижения их надежности и соответственно их стоимости в балансе предприятия) – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Аморт}}}$.
2. ***Эксплуатационные затраты*** на СОИБ (годовой бюджет ИБ без учета затрат на приобретение и установку СТЗИ-СОБИТ, на восстановление и ликвидацию последствий по инцидентам) – $TCO_{\text{СОИБ}}^{(\text{Экспл})}$, включая:
   - годовой бюджет на содержание штатных подразделений ИБ и должностей ИБ в других подразделениях (заработная плата персонала, другие расходы без учета стоимости приобретения СТЗИ-СОБИТ и обучения персонала по ИБ), в т.ч. затраты на аутсорсинг ИБ (функции SOC[13] внешними структурами и т.д.)[14] – $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{ЗП}}}$;
   - затраты на сопровождение, регламентное техническое обслуживание, ремонт СТЗИ-СОБИТ (программных и программно-аппаратных СТЗИ-СОБИТ, составляющих программно-техническую основу СОИБ)[15] – $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Сопр}}}$;
   - затраты на обучение (получение квалификационных категорий, повышение квалификации) персонала предприятия по вопросам ИБ (подразделений ИБ и других подразделений) в специализированных внешних и/или внутренних учебных структурах – $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Обуч}}}$;
   - затраты на предупредительно-профилактические мероприятия ИБ (аудит ИБ, в т.ч. активный аудит внешними структурами, т.е. проведение тестирования на проникновение, тренировки/учения по ИБ, проводимые внешними структурами) – $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Предупр}}}$.
3. ***Затраты (потери), связанные с целевой результативностью СОИБ*** (из-за инцидентов ИБ, ситуаций и процедур ИБ) – $TCO_{\text{СОИБ}}^{(\text{Рез})}$:
   - потери предприятия из-за остановки функционирования корпоративной информационной системы (ИС, АС, АСУТП, компьютерной сети, отдельных АРМ) в результате инцидентов ИБ – $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Остан}}}$;
   - затраты на восстановление функционирования корпоративной информационной системы (ее элементов) после инцидентов ИБ и ликвидацию других негативных последствий (репутационных, нормативных, социальных) – $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Вост}}}$;
   - стоимость (издержки) из-за потерь рабочего времени сотрудников и должностных лиц предприятия, связанных с административно-технологическими процедурами и ситуациями ИБ (время получения/изменения учетной записи и/или прав доступа, идентификационных атрибутов, т.е. паролей, электронных ключей в ИС, АС, АСУТП корпоративной информационной системы[16], время блокирования учетных записей пользователей в результате несоблюдения или игнорирования ими требований и процедур ИБ, их небрежности, невнимательности и т.п.) – $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{РабВр}}}$.

13 Security Operation Center.

14 Во многих источниках отдельно выделяют затраты на планирование мероприятий ИБ, на контроль состояния ИБ, на поддержание соответствия нормативным требованиям регуляторов, на пересмотр политик/угроз ИБ, локальной нормативной базы ИБ. Вместе с тем данные работы в основной своей массе выполняются сотрудниками подразделений ИБ и входят в группу затрат на их содержание (заработная плата персонала, годовые затраты на деятельность соответствующих подразделений без учета стоимости приобретения СЗИ-СОБИТ), т.е. отражаются в годовом бюджете по расходам, связанным с подразделением ИБ.

15 Причем как внешними организациями, так и внутренними структурными подразделениями (в рамках составляющих их бюджета по соответствующим расходам).

16 Следует отметить, что вообще говоря данные издержки следует относить к TCO_{IT} IT-сферы предприятия, поскольку они связаны с эффективностью деятельности системных администраторов, входящих в состав не ИБ, а IT-подразделений, но во многих случаях в соответствующих процедурах участвуют администраторы безопасности, что является основанием для учета соответствующих издержек и в $TCO_{\text{СОИБ}}$.

Таким образом:

$$TCO_{\text{СОИБ}} = TCO_{\text{СОИБ}}^{(\text{Кап})} + TCO_{\text{СОИБ}}^{(\text{Экспл})} + TCO_{\text{СОИБ}}^{(\text{Рез})} =$$
$$= TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}}} + TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Оргтех}}} + TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Аморт}}} +$$
$$+ TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{ЗП}}} + TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Сопр}}} + TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Обуч}}} +$$
$$+ TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Предупр}}} + TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Остан}}} + TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Вост}}} +$$
$$TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{РабВр}}}. \quad (10)$$

Представленная структура затрат на ИБ предприятия охватывает все составляющие системы обеспечения информационной безопасности, наглядна как для технических специалистов, так и для финансово-экономических работников, и дает полную детализированную картину расходов и затрат на ИБ для собственника (руководства) предприятия.

Важно отметить, что представленная структура затрат включает количественные показатели, которые в большинстве своем, как это показано работах Лукацкого А. В.[17], можно объективно фиксировать в системе внутриотчетной статистики и финансово-экономической документации предприятия.

Также следует отметить различие применяемого в анализах и обзорах по состоянию обеспечения ИБ на предприятиях и в организациях понятия «бюджет ИБ» $BD_{\text{ИБ}}$ от $TCO_{\text{СОИБ}}$ по соотношению (10). Как правило, бюджет ИБ включает эксплуатационные затраты на СОИБ (в нашем случае – $TCO_{\text{СОИБ}}^{(\text{Экспл})}$ и затраты на приобретение новых СТЗИ-СОБИТ, а также затраты по организационно-техническим мероприятиям на развитие СОИБ, осуществляемые в текущем году (в нашем случае – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}_{\text{Текущ}}}}$ и $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Оргтех}_{\text{Текущ}}}}$.

Таким образом бюджет предприятия на ИБ:

$$BD_{\text{ИБ}} = TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}_{\text{Текущ}}}} + TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Оргтех}_{\text{Текущ}}}} + TCO_{\text{СОИБ}}^{(\text{Экспл})}. \quad (11)$$

Кроме того, в целях нивелирования различий предприятий по масштабу бюджет ИБ $BD_{\text{ИБ}}$ как правило анализируется не столько в абсолютных значениях, а в относительной доле бюджета на IT-сферу предприятия.

Детальное рассмотрение параметров (метрик), отражающих, прежде всего результативно-целевую сторону создания и функционирования СОИБ ($TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Остан}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Вост}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{РабВр}}}$) представлено в отмеченных работах Лукацкого А. В. и работе Филиппова М. Г.[18]

17 Лукацкий А. В. Как посчитать эффективность информационной безопасности? [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ua/assets/securityforum/presentations/10_security_measurement.pdf (Дата обращения 12.08.25).

18 Филиппов М. Г. Сколько стоит безопасность. Анализ процессов обеспечения ИБ в российских компаниях. [Электронный ресурс]. URL: https://pt-corp.storage.yandexcloud.net/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (Дата обращения 12.08.25).

3. Целевая функция и экспертно аналитическая методика анализа технико экономической эффективности СОИБ по принципу сравнения с «лучшими практиками»

Оценка технико-экономической эффективности СОИБ предприятия на основе количественного сравнения $TCO_{\text{СОИБ}}$ с «лучшими практиками» или усредненными по отрасли значениями несмотря на свою логичность, информативность и наглядность, тем не менее характеризуется рядом проблем.

Во-первых, в интегральном показателе $TCO_{\text{СОИБ}}$ нивелируется «вклад» различных составляющих в эффективность СОИБ предприятия, поэтому требуется сравнивать с «лучшими практиками» или средними по отрасли показателями не только интегральный показатель $TCO_{\text{СОИБ}}$, но и осуществлять сравнительный анализ всех его слагаемых – $TCO_{\text{СОИБ}}^{(\text{Кап})}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})}$, $TCO_{\text{СОИБ}}^{(\text{Рез})}$, и, в свою очередь, их составляющих – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}}}$, $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Оргтех}}}$, $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{Аморт}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{ЗП}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Сопр}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Обуч}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Предупр}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Остан}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Вост}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{РабВр}}}$.

Во-вторых, количественная оценка эффективности СОИБ по принципу сравнения» с «лучшими практиками» или усредненными значениями может осуществляется различным образом, самым очевидным из которых является использование относительных значений[19] –

$$\left(\frac{TCO_{\text{СОИБ}}}{TCO_{\text{Предпр}}}\right) \Big/ \overline{\left(\frac{TCO_{\text{СОИБ}}}{TCO_{\text{Предпр}}}\right)}_{\text{Отрасл}}$$

или с учетом существенных различий $TCO_{\text{Предпр}}$ по отраслям, масштабу и специфике предприятий на основе сравнения с TCO_{IT} IT-сферы (IT-инфраструктуры) предприятия –

$$\left(\frac{TCO_{\text{СОИБ}}}{TCO_{\text{IT}}}\right) \Big/ \overline{\left(\frac{TCO_{\text{СОИБ}}}{TCO_{\text{IT}}}\right)}_{\text{Отрасл}}.$$

В этом случае наибольшая эффективность СОИБ предприятия характеризуется единичными значениями соответствующих отношений, но величина отклонения от единицы в большую или меньшую стороны трудно поддается интерпретации в качестве метрики эффективности.

В-третьих, как абсолютные, так и относительные значения $TCO_{\text{СОИБ}}$ и его составляющих по соотношению (10) не могут отражать специфику предприятия, в т.ч. одной отрасли, с точки зрения особенностей внутренней и внешней среды, т.н. «зрелости» бизнес-процессов, инфраструктуры и т.д. Иначе говоря отклонение $TCO_{\text{СОИБ}}$ от среднего значения на 20 % для одного (специфичного) предприятия может означать высокую эффективность СОИБ, а для другого (типового) недостаточную эффективность.

19 *Обозначение $(\overline{x})_{\text{отрасл}}$ означает среднее значение величины x по отрасли.*

В-четвертых, несмотря на то, что представленная структура затрат на СОИБ по соотношению (10), как отмечалось, включает количественные показатели, все же в отношении таких составляющих, как стоимость ликвидации репутационных (нормативных, социальных) негативных последствий ($ТСО^{(Рез)_{Вост_{Репутац}}}_{СОИБ}$) от компьютерных инцидентов, имеется существенная неопределенность в количественных методиках их подсчета. В этом же плане имеются трудности и неопределенности с определением величины $ТСО^{(Рез)_{РабВр}}_{СОИБ}$, поскольку несмотря на показанную Лукацким А. В. возможность создания систем внутренней отчетности, которые фиксируют и учитывают потери рабочего времени из-за процедур ИБ (блокирование учетных записей пользователей в результате несоблюдения или игнорирования ими требований и процедур ИБ и соответствующие обращения в подразделения ИБ или Service Desk для их разрешения и т.п.), все же часть потерь рабочего времени связана с самостоятельным решением (попытками) пользователями соответствующих проблем и трудно фиксируется в системах учета и отчетности.

Разрешением отмеченных проблем может стать использование экспертных оценок в процессах сравнения составляющих $ТСО_{СОИБ}$ с «лучшими практиками» или средними по отрасли значениями с учетом специфики конкретного предприятия и введение на этой основе суперпозиционной целевой функции технико-экономической эффективности СОИБ.

Суть представляемого подхода заключается в следующем.

В качестве целевой функции $ТЭЭ_{СОИБ}$ технико-экономической эффективности СОИБ рассматривается взвешенное суммирование показателей технико-экономической эффективности по составляющим затрат на СОИБ, установленным соотношением (10):

$$ТЭЭ_{СОИБ} = c_{(Кап)} ТЭЭ^{(Кап)}_{СОИБ} + c_{(Экспл)} ТЭЭ^{(Экспл)}_{СОИБ} + c_{(Рез)} ТЭЭ^{(Рез)}_{СОИБ} = c_{(Кап)} \left(c_{(Кап)_{СТЗИ}} ТЭЭ^{(Кап)_{СТЗИ}}_{СОИБ} + c_{(Кап)_{Оргтех}} ТЭЭ^{(Кап)_{Оргтех}}_{СОИБ} + c_{(Кап)_{Аморт}} ТЭЭ^{(Кап)_{Аморт}}_{СОИБ} \right) + c_{(Экспл)} \left(c_{(Экспл)_{ЗП}} ТЭЭ^{(Экспл)_{ЗП}}_{СОИБ} + c_{(Экспл)_{Сопр}} ТЭЭ^{(Экспл)_{Сопр}}_{СОИБ} + c_{(Экспл)_{Обуч}} ТЭЭ^{(Экспл)_{Обуч}}_{СОИБ} + c_{(Экспл)_{Предупр}} ТЭЭ^{(Экспл)_{Предупр}}_{СОИБ} \right) + c_{(Рез)} \left(c_{(Рез)_{Остан}} ТЭЭ^{(Рез)_{Остан}}_{СОИБ} + c_{(Рез)_{Вост}} ТЭЭ^{(Рез)_{Вост}}_{СОИБ} + c_{(Рез)_{РабВр}} ТЭЭ^{(Рез)_{РабВр}}_{СОИБ} \right), \quad (12)$$

где

- $ТЭЭ^{(Кап)}_{СОИБ}$, $ТЭЭ^{(Экспл)}_{СОИБ}$, $ТЭЭ^{(Рез)}_{СОИБ}$, $ТЭЭ^{(Кап)_{СТЗИ}}_{СОИБ}$, $ТЭЭ^{(Кап)_{Оргтех}}_{СОИБ}$, $ТЭЭ^{(Кап)_{Аморт}}_{СОИБ}$, $ТЭЭ^{(Экспл)_{ЗП}}_{СОИБ}$, $ТЭЭ^{(Экспл)_{Сопр}}_{СОИБ}$, $ТЭЭ^{(Экспл)_{Обуч}}_{СОИБ}$, $ТЭЭ^{(Экспл)_{Предупр}}_{СОИБ}$, $ТЭЭ^{(Рез)_{Остан}}_{СОИБ}$, $ТЭЭ^{(Рез)_{Вост}}_{СОИБ}$, $ТЭЭ^{(Рез)_{РабВр}}_{СОИБ}$ – величины технико-экономической эффективности СОИБ по составляющим структуры затрат на СОИБ первого и второго уровня детализации, соответственно;
- $(c_{(Кап)} + c_{(Экспл)} + c_{(Рез)} = 1)$ – весовые коэффициенты относительной значимости влияния капитальных, эксплуатационных и результативно-целевых составляющих затрат на интегральный показатель технико-экономической эффективности СОИБ $ТЭЭ_{СОИБ}$;
- $(c_{(Кап)_{СТЗИ}} + c_{(Кап)_{Оргтех}} + c_{(Кап)_{Аморт}}) = 1)$ – весовые коэффициенты относительной значимости влияния составляющих капитальных затрат на $ТЭЭ^{(Кап)}_{СОИБ}$;
- $(c_{(Экспл)_{ЗП}} + c_{(Экспл)_{Сопр}} + c_{(Экспл)_{Обуч}} + c_{(Экспл)_{Предупр}}) = 1$ – весовые коэффициенты относительной значимости влияния составляющих эксплуатационных затрат на $ТЭЭ^{(Экспл)}_{СОИБ}$;
- $(c_{(Рез)_{Остан}} + c_{(Рез)_{Вост}} + c_{(Рез)_{РабВр}})$ – весовые коэффициенты относительной значимости влияния составляющих затрат, связанных с результативно-целевой стороной СОИБ, на $ТЭЭ^{(Рез)}_{СОИБ}$.

Введение целевой функции (12) позволяет сформировать следующую Методику экспертно-аналитического анализа технико-экономической эффективности системы обеспечения информационной безопасности предприятия по принципу сравнения с «лучшими практиками».

1. На основе внутренней статистической отчетности и финансово-экономической документации предприятия определяются количественные значения составляющих капитальных, эксплуатационных затрат и затрат, связанных с результативно-целевой стороной по функционированию СОИБ, – $ТСО^{(Кап)}_{СОИБ}$, $ТСО^{(Экспл)}_{СОИБ}$, $ТСО^{(Рез)}_{СОИБ}$, $ТСО^{(Кап)_{СТЗИ}}_{СОИБ}$, $ТСО^{(Кап)_{Оргтех}}_{СОИБ}$, $ТСО^{(Кап)_{Аморт}}_{СОИБ}$, $ТСО^{(Экспл)_{ЗП}}_{СОИБ}$, $ТСО^{(Экспл)_{Сопр}}_{СОИБ}$, $ТСО^{(Экспл)_{Обуч}}_{СОИБ}$, $ТСО^{(Экспл)_{Предупр}}_{СОИБ}$, $ТСО^{(Рез)_{Остан}}_{СОИБ}$, $ТСО^{(Рез)_{Вост}}_{СОИБ}$, $ТСО^{(Рез)_{РабВр}}_{СОИБ}$.

2. На основе экспертных оценок специалистов, хорошо представляющих специфику деятельности предприятия, ее IT-сферы (IT-инфраструктуры), приоритеты бизнеса и общую политику безопасности предприятия, включая политику информационной безопасности, определяются весовые коэффициенты $c_{(Кап)}$, $c_{(Экспл)}$, $c_{(Рез)}$, $c_{(Кап)_{СТЗИ}}$, $c_{(Кап)_{Оргтех}}$, $c_{(Кап)_{Аморт}}$, $c_{(Экспл)_{ЗП}}$, $c_{(Экспл)_{Сопр}}$, $c_{(Экспл)_{Обуч}}$, $c_{(Экспл)_{Предупр}}$, $c_{(Рез)_{Остан}}$, $c_{(Рез)_{Вост}}$, $c_{(Рез)_{РабВр}}$.

3. Эксперты на основе сравнения количественных значений составляющих $ТСО_{СОИБ}$ (см. п. 1) с аналогичными значениями «лучших практик» или со средними значениями по отрасли соответствующих показателей и учитывая специфику предприятия с точки зрения особенностей внутренней и внешней среды, «зрелости» бизнес-процессов и инфраструктуры и т.д. в порядково-вербальной шкале Харрингтона[20] (см. табл. 1) выставляют качественные

20 Мацкевич А. А. Управленческие шкалы. Часть 1. Шкалы показателей без планового значения // Управление предприятием. [Электронный ресурс]. URL: https://upr.ru/article/upravlencheskie-shkaly-chast-1-shkaly-pokazateley-bez-planovogo-znacheniya/ (Дата обращения 12.08.25).

(порядковые) оценки соответствующих показателей технико-экономической эффективности СОИБ[21] – $[\widehat{ТЭЭ}]^{(Кап)_{СТЗИ}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Кап)_{Оргтех}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Кап)_{Аморт}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Экспл)_{ЗП}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Экспл)_{Сопр}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Экспл)_{Обуч}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Экспл)_{Предупр}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Рез)_{Остан}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Рез)_{Вост}}_{СОИБ}$, $[\widehat{ТЭЭ}]^{(Рез)_{РабВр}}_{СОИБ}$.

Другим вариантом может быть использование шкалы экспертного сравнения альтернатив Т. Саати[22] (см. табл. 2). Эксперты в контексте технико-экономической эффективности СОИБ сравнивают две альтернативы – количественные значения соответствующих составляющих $ТСО_{СОИБ}$ предприятия (первая альтернатива) и усредненных значений по отрасли соответствующих значений составляющих $ТСО_{СОИБ}$ (вторая альтернатива).

4. Формируются усредненные экспертные оценки составляющих $ТЭЭ_{СОИБ}$ в порядковой шкале путем взятия медианы ряда индивидуальных экспертных оценок, выстроенных в неубывающей последовательности[23] – $\left([\widehat{ТЭЭ}]^{(Кап)_{СТЗИ}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Кап)_{Оргтех}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Кап)_{Аморт}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Экспл)_{ЗП}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Экспл)_{Сопр}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Экспл)_{Обуч}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Экспл)_{Предупр}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Рез)_{Остан}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Рез)_{Вост}}_{СОИБ}\right)_{Усред}$, $\left([\widehat{ТЭЭ}]^{(Рез)_{РабВр}}_{СОИБ}\right)_{Усред}$.

5. На основе соотношения порядковых и балльных оценок, установленных в шкале Харрингтона или шкале Т. Саати, усредненные экспертные оценки составляющих технико-экономической эффективности СОИБ в порядковой шкале переводятся в числовую шкалу [0,1] по шкале Харрингтона (см. табл. 1) или в бальные оценки по шкале Т. Саати[24] (см. табл. 2) – $\left(\overline{ТЭЭ}^{(Кап)_{СТЗИ}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Кап)_{Оргтех}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Кап)_{Аморт}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Экспл)_{ЗП}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Экспл)_{Сопр}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Экспл)_{Обуч}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Экспл)_{Предупр}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Рез)_{Остан}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Рез)_{Вост}}_{СОИБ}\right)_{Усред}$, $\left(\overline{ТЭЭ}^{(Рез)_{РабВр}}_{СОИБ}\right)_{Усред}$.

6. По соотношению (12) на основе весового суммирования с соответствующими весовыми коэффициентами по количественным усредненным экспертным оценкам, полученным по п. 5, определяются величины технико-экономической эффективности СОИБ в разрезе ее трех составляющих – $\overline{ТЭЭ}^{(Кап)}_{СОИБ}$, $\overline{ТЭЭ}^{(Экспл)}_{СОИБ}$, $\overline{ТЭЭ}^{(Рез)}_{СОИБ}$ и интегральный показатель $\overline{ТЭЭ}_{СОИБ}$.

С учетом единичной нормировки весовых коэффициентов максимальное значение величин $\overline{ТЭЭ}^{(Кап)}_{СОИБ}$, $\overline{ТЭЭ}^{(Экспл)}_{СОИБ}$, $\overline{ТЭЭ}^{(Рез)}_{СОИБ}$ и $\overline{ТЭЭ}_{СОИБ}$ в шкале Харрингтона равняется единице (100 %), в шкале Т. Саати равняется девяти (100 %).

Таблица 1.

Шкала Харрингтона

Порядково-вербальное значение оцениваемой величины	Числовое значение в шкале [0,1]
Очень высокое	[0,8 – 1]
Высокое	[0,64 – 0,8]
Среднее	[0,37 – 0,64]
Низкое	[0,2 – 0,37]
Очень низкое	[0 – 0,2]

Следует отметить, что на стратегическом уровне анализа эффективности деятельности предприятия оценки интегральных показателей технико-экономической эффективности $\overline{ТЭЭ}^{(Кап)}_{СОИБ}$, $\overline{ТЭЭ}^{(Экспл)}_{СОИБ}$, $\overline{ТЭЭ}^{(Рез)}_{СОИБ}$ и $\overline{ТЭЭ}_{СОИБ}$ помимо количественной (бальной, процентной) шкалы могут требоваться и обратно в порядко-вербальной шкале. Такие оценки формируются обратным преобразованием по шкалам Харрингтона или Т. Саати.

Проиллюстрируем на примере гипотетического предприятия результаты экспертно-аналитической оценки технико-экономической эффективности СОИБ по представленной методике[25], которые для наглядности сведены в табл. 3.

Приведенный пример-иллюстрация наглядно раскрывает «картину» составляющих технико-экономической эффективности СОИБ и особенности экспертно-аналитического характера представленной методики.

В первую очередь следует отметить необходимость создания и ведения баз данных по используемым в методике среднестатистическим показателям –

$$\left(\overline{ТСО}^{(Кап)_{СТЗИ}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Кап)_{Оргтех}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Кап)_{Аморт}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Экспл)_{ЗП}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Экспл)_{Сопр}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Экспл)_{Обуч}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Экспл)_{Предупр}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Рез)_{Остан}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Рез)_{Вост}}_{СОИБ}\right)_{Отрасл}, \left(\overline{ТСО}^{(Рез)_{РабВр}}_{СОИБ}\right)_{Отрасл}$$

в разрезе разных отраслей предприятий и организаций. Насколько известно, такие базы данных, но в отношении $ТСО_{IT}$, ведут известные консалтинго-исследовательские в сфере IT-компании, в частности Gartner Group. На российском рынке исследованиями

21 Обозначение $[\hat{x}]$ в данном случае означает оценку величины x в порядковой (вербальной) шкале Харрингтона.

22 Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. 278 с.

23 Усреднение индивидуальных экспертных оценок в порядковой шкале путем взятия медианы их неубывающего ряда является корректной математической операцией усреднения. Пример: пусть 7 экспертов величине x дали следующие индивидуальные оценки в порядковой шкале – $[\hat{x}]_1$ = «низкая», $[\hat{x}]_2$ = «высокая», $[\hat{x}]_3$ = «средняя», $[\hat{x}]_4$ = «низкая», $[\hat{x}]_5$ = «низкая», $[\hat{x}]_6$ = «низкая», $[\hat{x}]_7$ = «средняя»; выстраивая индивидуальные оценки в неубывающий ряд – («низкая», «низкая», «низкая», «низкая», «средняя», «средняя», «высокая») по его медиане (середине) получаем усредненную экспертную оценку в порядковой шкале $[\hat{x}]_{усред}$ = «низкая».

24 Обозначение $\hat{x}$ означает оценку величины x в количественной (интервальной) шкале значений.

25 Среднестатистические показатели в табл. 3 не имеют отношения к реальной действительности, являются гипотетическими и используются исключительно для иллюстрации. Все весовые коэффициенты для слагаемых целевой функции $ТЭЭ_{СОИБ}$ одинаковы, т.е. равны 1/3 или 1/4 для коэффициентов $\overline{ТЭЭ}^{(Экспл)}_{СОИБ}$.

Таблица 2.

Шкала сравнения альтернатив Т. Саати

Порядково-вербальная оценка предпочтительности альтернативы	Соответствующая балльная оценка	Пояснение (квалиметрическая характеристика)
Абсолютное превосходство (гораздо хуже)	9 (1/9)	Альтернатива абсолютно (неоспоримо) предпочтительнее, весь опыт эксперта и многочисленная практика в высшей степени убедительно свидетельствуют об этом
Значительное превосходство (значительно хуже)	7 (1/7)	Альтернатива значительно (убедительно, совершенно очевидно) предпочтительнее, опыт эксперта и известная эксперту практика свидетельствуют об этом
Существенное (сильное) превосходство (хуже)	5 (1/5)	Альтернатива существенно (явно) предпочтительнее, имеются свидетельства и надежные данные в пользу этого решения
Среднее (слабое) превосходство (чуть хуже)	3 (1/3)	Альтернатива незначительно (немного) предпочтительнее, имеется некоторый опыт и некоторые свидетельства в пользу такого решения, но они недостаточно убедительны
Несравнимы	0	По анализируемому свойству альтернативы несравнимы (разной природы) или эксперт затрудняется в сравнении альтернатив, поскольку не имеется никакого опыта, никаких свидетельств в пользу превосходства одной альтернативы над другой
Промежуточные решения	2, 4, 6, 8 (1/2, 1/4, 1/6, 1/8)	

Таблица 3.

Иллюстративный пример экспертно-аналитической оценки технико экономической эффективности СОИБ

Частные показатели эффективности СОИБ		Среднестатистические показатели затрат на СОИБ по группе однородных предприятий	Показатели СОИБ конкретного предприятия	Усредненная экспертная оценка эффективности СОИБ по соответствующим показателям на основе сравнения со среднестатистическими (с «best practices»)	
				Порядковые оценки по шкале Т. Саати	Баллы по шкале Т. Саати
1		2	3	4	5
$\widehat{ТЭЭ}^{(Кап)}_{СОИБ}$	По капитальным затратам на создание СОИБ				
	$\widehat{ТЭЭ}^{(Кап)_{СТЗИ}}_{СОИБ}$	По затратам на приобретение и установку СТЗИ-СОБИТ, % от стоимости программно-технических средств КИС (корпоративная информационная система)			
		15 %	20 %	Существенно лучше	5
	$\widehat{ТЭЭ}^{(Кап)_{Оргтех}}_{СОИБ}$	По затратам на организационно-технические и организационно-штатные мероприятия в рамках создания СОИБ, % от общих расходов предприятия			
		3 %	1 %	Значительно хуже	1/7
	$\widehat{ТЭЭ}^{(Кап)_{Аморт}}_{СОИБ}$	По годовым показателям амортизации стоимости СТЗИ-СОБИТ и технологий СОИБ (% ежегодного уменьшения стоимости основных средств, устаревание технологий)			
		30 %	25 %	Чуть лучше	3
ИТОГО (баллы) $\widehat{ТЭЭ}^{(Кап)}_{СОИБ} = c_{(Кап)_{СТЗИ}} \widehat{ТЭЭ}^{(Кап)_{СТЗИ}}_{СОИБ} + c_{(Кап)_{Оргтех}} \widehat{ТЭЭ}^{(Кап)_{Оргтех}}_{СОИБ} + c_{(Кап)_{Аморт}} \widehat{ТЭЭ}^{(Кап)_{Аморт}}_{СОИБ}$					**2,7**
ИТОГО (%) $\widehat{ТЭЭ}^{(Кап)}_{СОИБ}$ = **30 %** (от максимальной или оптимальной по отрасли) ИТОГО (по шкале Саати) $[\widehat{ТЭЭ}]^{(Кап)}_{СОИБ}$ = «**Средняя**» (относительно оптимальной по отрасли)					

1		2	3	4	5
$\widehat{ТЭЭ}^{(Экспл)}_{СОИБ}$	По эксплуатационным затратам на СОИБ				
	$\widehat{ТЭЭ}^{(Экспл)_{ЗП}}_{СОИБ}$	По заработной плате персонала подразделений СОИБ, включая затраты на аутсорсинг ИБ (SOC и т.д. кроме пентестинга), % от ФОТ предприятия			
		3 %	5 %	Существенно лучше	5
	$\widehat{ТЭЭ}^{(Экспл)_{Сопр}}_{СОИБ}$	По затратам на сопровождение, регламентное техническое обслуживание, ремонт СТЗИ-СОБИТ, % от стоимости СТЗИ-СОБИТ			
		12 %	20 %	Значительно лучше	7
	$\widehat{ТЭЭ}^{(Экспл)_{Обуч}}_{СОИБ}$	По затратам на обучение персонала предприятия по вопросам ИБ, % от годового дохода предприятия			
		0,035 %	0,03 %	Средне	3
	$\widehat{ТЭЭ}^{(Экспл)_{Предупр}}_{СОИБ}$	Затраты на предупредительно-профилактические мероприятия ИБ (аудит, пентестинг, учения/тренировки), % от бюджета на ИБ (от $BD_{ИБ}$)			
		10 %	15 %	Значительно лучше	7
ИТОГО (баллы) $\widehat{ТЭЭ}^{(Экспл)}_{СОИБ} = c_{(Экспл)_{ЗП}} \widehat{ТЭЭ}^{(Экспл)_{ЗП}}_{СОИБ} + c_{(Экспл)_{Сопр}} \widehat{ТЭЭ}^{(Экспл)_{Сопр}}_{СОИБ} + c_{(Экспл)_{Обуч}} \widehat{ТЭЭ}^{(Экспл)_{Обуч}}_{СОИБ} + c_{(Экспл)_{Предупр}} \widehat{ТЭЭ}^{(Экспл)_{Предупр}}_{СОИБ}$					**5,5**
ИТОГО (%) $\widehat{ТЭЭ}^{(Экспл)}_{СОИБ}$ = **61 %** (от максимальной или оптимальной по отрасли) ИТОГО (по шкале Саати) $[\widehat{ТЭЭ}]^{(Экспл)}_{СОИБ}$ = «**Значительно лучше средней**» (по отрасли)					
$\widehat{ТЭЭ}^{(Рез)}_{СОИБ}$	По затратам/потерям в отношении результативно-целевой составляющей СОИБ				
	$\widehat{ТЭЭ}^{(Рез)_{Остан}}_{СОИБ}$	По потерям из-за остановки функционирования корпоративной информационной системы (ИС, АС, АСУТП, компьютерной сети, отдельных АРМ) в результате инцидентов ИБ, % от годового дохода предприятия			
		2 %	1 %	Существенно лучше	5
	$\widehat{ТЭЭ}^{(Рез)_{Вост}}_{СОИБ}$	По затратам на восстановление функционирования корпоративной информационной системы после инцидентов ИБ и ликвидацию других негативных последствий (репутационных, нормативных, социальных), % от годового дохода предприятия			
		1 %	1,5 %	Существенно хуже	1/5
	$\widehat{ТЭЭ}^{(Рез)_{РабВр}}_{СОИБ}$	Потери рабочего времени сотрудников предприятия, связанные с административно-технологическими процедурами ИБ (из-за блокирования учетных записей и т.п.), % от годового бюджета рабочего времени предприятия			
		2 %	1 %	Значительно лучше	7
ИТОГО (баллы) $\widehat{ТЭЭ}^{(Рез)}_{СОИБ} = c_{(Рез)_{Остан}} \widehat{ТЭЭ}^{(Рез)_{Остан}}_{СОИБ} + c_{(Рез)_{Вост}} \widehat{ТЭЭ}^{(Рез)_{Вост}}_{СОИБ} + c_{(Рез)_{РабВр}} \widehat{ТЭЭ}^{(Рез)_{РабВр}}_{СОИБ}$					**4,07**
ИТОГО (%) $\widehat{ТЭЭ}^{(Рез)}_{СОИБ}$ = **45 %** (от максимальной или оптимальной по отрасли) ИТОГО (по шкале Саати) $[\widehat{ТЭЭ}]^{(Рез)}_{СОИБ}$ = «**Значительно лучше средней**» (по отрасли)					
ИТОГО по общей (интегральной) технико-экономической эффективности СОИБ предприятия, баллы: $\widehat{ТЭЭ}_{СОИБ} = c_{(Кап)} \widehat{ТЭЭ}^{(Кап)}_{СОИБ} + c_{(Экспл)} \widehat{ТЭЭ}^{(Экспл)}_{СОИБ} + c_{(Рез)} \widehat{ТЭЭ}^{(Рез)}_{СОИБ}$					**4,39**
ИТОГО общая (интегральная) технико-экономическая эффективность СОИБ предприятия (%): $\widehat{ТЭЭ}_{СОИБ}$ = **49 %** (от максимальной или оптимальной по отрасли)					
ИТОГО (по шкале Саати) общая (интегральная) технико-экономическая эффективность СОИБ предприятия: $[\widehat{ТЭЭ}]_{СОИБ}$ = «**Немного лучше средней**» (по отрасли)					

в сфере эффективности затрат (бюджетов) на информационную безопасность предприятий помимо отдельных известных специалистов (Лукацкий А. В.) занимается также ряд ведущих в сфере ИБ компаний (Positive Technologies, Лаборатория Касперского, InfoWatch, РТК-Солар и др.). Источниками создания и ведения таких баз данных могут быть как материалы государственной статистики, так и специализированные опросы-исследования предприятий.

Кроме того, в представленной методике принципиальным являются экспертные оценки показателей технико-экономической эффективности, осуществляемые экспертами на основе количественных сравнений.

У многих специалистов-практиков наблюдается устойчивый скепсис в отношении экспертных оценок из-за их якобы неотъемлемой субъективности. Очевидно, это происходит в результате непонимания сути и особенностей организационно-процедурной стороны экспертных оценок. При правильно сформированной экспертной группе, качественно разработанных оценочных инструментах (опросных листах), профессионально организованных процедурах опроса экспертов и корректной математической обработке результатов индивидуальных оценок процедуры экспертных оценок позволяют решать «нерешаемые» (не формализуемые или трудно-формализуемые) задачи и проблемы, обеспечивают высокую степень объективности итоговых оценок, что широко известно и активно применяется в сфере выработки и принятия управленческих решений [20].

В отношении данной методики экспертные оценки не только позволяют свести все показатели технико-экономической эффективности СОИБ в единую шкалу, но при сравнении количественных показателей предприятия и среднестатистических отраслевых показателей обеспечивают учет существенной во многих случаях специфики или наоборот типичности инфраструктуры конкретного предприятия, кадрового обеспечения, бизнес-политики и политики ИБ.

Заключение

Представленные целевая функция и экспертно-аналитическая методика анализа технико-экономической эффективности СОИБ базируются на классической структуре широко известного и применяемого технико-экономического показателя «TCO» (total cost of ownership), но специфицированного в отношении обеспечивающего характера сферы ИБ в отношении в свою очередь обеспечивающей основную деятельность предприятия IT сферы. Исходя из этого, общий смысл и детализация показателей технико-экономической эффективности СОИБ, как представляется, должны быть хорошо понимаемыми и наглядными для руководителей и финансово-экономических работников предприятий, что является, в свою очередь информативной основой для руководителей СОИБ при формировании и «отстаивании» бюджетов ИБ.

Часть показателей $TCO_{\text{СОИБ}}$ второго уровня детализации фиксируется и ведется в системе внутренней отчетности и финансово-экономической документации предприятий – $TCO_{\text{СОИБ}}^{(\text{Кап})_{\text{СТЗИ}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{ЗП}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Сопр}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Обуч}}}$, $TCO_{\text{СОИБ}}^{(\text{Экспл})_{\text{Предупр}}}$. Другая часть ($TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Остан}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{Вост}}}$, $TCO_{\text{СОИБ}}^{(\text{Рез})_{\text{РабВр}}}$), как это показано в обстоятельных работах Лукацкого А. В., может формироваться в специально создаваемой на предприятии системе учета в сфере функционирования СОИБ.

Вместе с тем, как уже указывалось, требуется создание и ведение баз данных по используемым в методике среднестатистическим показателям $TCO_{\text{СОИБ}}$ в разрезе отраслей предприятий и организаций, что может быть одной из специализаций консалтингово-исследовательских компаний в сфере ИБ.

Литература

1. Паршина И. С. Рентабельность инвестиций (ROI) в проекты внедрения исполнительных производственных систем (MES) на российских предприятиях // Наукоемкие технологии в машиностроении. 2020. № 3 (105). С. 37–43.
2. Zelezinskii et al. Modern Methods of Evaluating the Effectiveness of the Organization // Экономический вектор 2021. № 4(27). pp. 65–70.
3. Zegzhda D. P., Saurenko T. N., Anisimov V. G., Anisimov E. G. Assessment of the Effectiveness of an Information Security System // Automatic Control and Computer Sciences. 2023. Volume 57, № 8. pp. 855–861. https://doi.org/10.3103/S0146411623080345.
4. Митяков Е. С., Артемова С. В., Бакаев А. А., Душкин А. В., Вегера Ж. Г. Модель оценки эффективности систем защиты информации // Безопасность информационных технологий. 2024. Том 31, № 4. С. 56–66. doi: 10.26583/bit.2024.4.03.
5. Belov V., Belova N., Pestunova T., Kosov D. Technique for Evaluating the Effectiveness of the Information Security Department. IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). 2023. pp. 1130–1133. DOI: 10.1109/APEIE59731.2023.10347645.
6. Сухов А. М., Крупенин А. В., Якунин В. И. Метод вычисления показателя эффективности процесса функционирования системы обеспечения информационной безопасности // Автоматизация процессов управления. 2022. № 1(67). С. 33–42.
7. Добрышин М. М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности // Известия тульского государственного университета. Технические науки. 2021. № 9. С. 113–121.
8. Sow M. et al. Evaluating Information Security System Effectiveness for Risk Management, Control, and Corporate Governance // Business and Economic Research. 2019. Vol. 9, № 1. pp.164–172.
9. Громов Ю. Ю., Карасев П. И., Губсков Ю. А., Котюкова В. О. Оценка эффективности систем защиты и анализ рисков информационной безопасности // Информация и безопасность. 2022. Т. 25, Вып. 2. С. 187–192.

10. Пашков Н. Н., Дрозд В. Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1. [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 26.08.2025).
11. Краузе Р. П. Исследование методических подходов к оценке эффективности ИТ-проектов на предприятиях // Бизнес-образование в экономике знаний. 2020. № 3. С.87–92.
12. Шабуров А. С., Шлыков А. И. Разработка метода оценки экономической эффективности системы защиты информации для коммерческих предприятий // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2020. № 36. С. 193–213.
13. Курило А. П., Паршин И. С., Симачков С. А., Потапов Г. Д. Определение эффективности комплексных систем обеспечения информационной безопасности методом экспертных оценок / Актуальные проблемы защиты информации: современность и перспективы. Материалы II Научно-практической конференции. Москва, 2025. С. 43–48.
14. Бутусов И. В., Нащекин П. А., Романов А. А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности. 2016. № 1(14). С. 9–16.
15. Ziro A., Gnatyuk S., Toibayeva S. Investigation of the Method of Evaluating the Effectiveness of the Information Security System Based on Fuzzy Inference // Scientific Journal of Astana IT University. 2023. Volume 13. pp. 52–63. DOI: 10.37943/13dzev3953.
16. Братченко А. И., Бутусов И. В., Кобелян А. М., Романов А. А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. 2019. № 1(29). С. 18–24.
17. Ермаков С. А., Чурсин А. Г., Болгов А. А. Нечетко-множественная методика оценки рисков автоматизированной системы «умный дом» с динамической топологией // Информация и безопасность. 2022. Т. 25. Вып. 4. С. 495–500.
18. Wojtaszek H. et al. Methods for Assessing the Economic Efficiency of IT Projects // European research studies journal. 2024. Volume XXVII (Issue 3). pp. 637–651. DOI:10.35808/ersj/3457.
19. Kasim M. K. M. et al. A systematic literature review on the effect of information systems on the performance of government officials International // Journal of Advanced and Applied Sciences, 11(3) 2024, Pages: 46–54.
20. Иванова Л. Н., Луговской В. Д. Экспертные оценки в принятии управленческих решений // Современные научные исследования и инновации. 2020. № 10 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/10/93677 (дата обращения: 26.08.2025).

METHODOLOGY OF EXPERT-ANALYTICAL ANALYSIS OF TECHNICAL AND ECONOMIC EFFICIENCY OF THE INFORMATION SECURITY SYSTEM OF AN ENTERPRISE BASED ON COMPARISON WITH «BEST PRACTICES»

Gaydamakin N. A.[26]

Keywords: *: information security management system, effectiveness, total cost of ownership, risk-based analysis, technical and economic analysis, expert and analytical analysis, costs of ensuring information security.*

Purpose of the study: *to consider methods for analyzing the effectiveness of information security systems of enterprises and to develop a methodology for expert-analytical analysis of their technical and economic efficiency based on comparison «with best practices».*

Methods of research: *application of methods for analyzing the efficiency of the IT sphere of enterprises based on the principles of «total cost of ownership».*

Result(s): *The problems of two main approaches to the analysis of the effectiveness of information security systems of enterprises – risk-based and techno-economic - are considered and analyzed.*

Based on the analysis of technical and economic efficiency according to the principle of «total cost of ownership» in the field of information technology, a systematization of expenses (costs) for ensuring the information security of the enterprise was carried out in the form of a two-level hierarchical scheme – capital costs (according to the cost of acquiring and installing technical means of information protection and means of ensuring the security of information technologies, costs of carrying out organizational-technical and organizational-staffing measures, depreciation losses), operating costs (for wages and outsourcing, for support and technical maintenance, for personnel training, for preventive and preventive measures in the form of audit, pentesting, training and exercises), costs and losses associated with the result-target side of the information security system (losses from downtime of the corporate information system as a result of computer incidents, costs of its restoration, loss of working time on organizational and technological procedures for information protection in the form of time spent on identification and authentication procedures, blocking of automated workstations as a result of incorrect actions of users).

The objective function of technical and economic efficiency of the information security system is presented based on the weighted summation of efficiency indicators for the components of the presented cost scheme, compared with «best practices» or average statistical values for the enterprise industry.

26 Nikolay A. Gaydamakin, Dr.Sc. (of Tech.), Professor, Ural Federal Boris Yeltsin University. Yekaterinburg, Russia. E-mail: n.a.gaidamakin@urfu.ru

A methodology has been developed for analyzing the technical and economic efficiency of enterprise information security systems based on the presented objective function and the application of the expert assessment method to take into account the specifics of enterprises in terms of IT infrastructure, business policy and information security policy. According to the formed methodology, an illustrative example of the results of the analysis of the technical and economic efficiency of the information security system of the enterprise is given.

Scientific novelty: *the systematization of costs, expenses and losses for ensuring information security in the methodology of «total cost of ownership» was carried out, a superposition objective function was proposed and an expert-analytical methodology based on it for analyzing the technical and economic efficiency of information security systems was proposed.*

References

1. Parshina I. S. Rentabel'nost' investitsiy (ROI) v proyekty razvitiya ispolnitel'nykh proizvodstvennykh sistem (IPS) na rossiyskikh predpriyatiyakh // Naukoyemkiye tekhnologii v ma-shinostroyenii. 2020. № 3(105). S. 37–43.
2. Zelezinskii et al. Modern Methods of Evaluating the Effectiveness of the Organization // Экономический вектор 2021. № 4(27). С. 65–70.
3. Zegzhda D. P., Saurenko T. N., Anisimov V. G., Anisimov E. G. Assessment of the Effectiveness of an Information Security System // Automatic Control and Computer Sciences. 2023. Volume 57, № 8. Pp. 855–861. https://doi.org/10.3103/S0146411623080345.
4. Mityakov E. S., Artemova S. V., Bakaev A. A., Dushkin A. V., Vegera Zh. G. Model for assessing the effectiveness of information security systems // Information Technology Security. 2024. Vol. 31, No. 4. Pp 56–66. doi: 10.26583/bit.2024.4.03.
5. Belov V., Belova N., Pestunova T., Kosov D. Technique for Evaluating the Effectiveness of the Information Security Department. IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE). 2023. Pp. 1130–1133. DOI: 10.1109/APEIE59731.2023.10347645.
6. Sukhov A. M., Krupenin A. V., Yakunin V. I. Metod rascheta effektivnosti effektivnogo protsessa preobrazovaniya obespecheniya informatsionnoy bezopasnosti // Avtomatizatsiya protsessov upravleniya. 2022. № 1(67). S. 33–42.
7. Dobryshin M. M. Podkhod k formirovaniyu obobshchennogo kriteriya effektivnosti effektivno-sti sistemy obespecheniya informatsionnoy bezopasnosti // Izvestiya tul'skogo gosu-darstvennogo universiteta. Tekhnicheskiye nauki. 2021. № 9. S. 113–121.
8. Sow M. et al. Evaluating Information Security System Effectiveness for Risk Management, Control, and Corporate Governance // Business and Economic Research. 2019. Vol. 9, № 1. Pp. 164–172.
9. Gromov YU. YU., Karasev P. I., Gubskov YU. A., Kotyukova V. O. Otsenka effektivnosti si-stem zashchity i analiz riskov informatsionnoy bezopasnosti // Informatsiya i bezopasnost'. 2022. T. 25, Vyp 2. S. 187–192.
10. Pashkov N. N., Drozd V. G. Analiz riskov informatsionnoy bezopasnosti i otsenki effektivnosti sistem zashchity informatsii na predpriyatii // Sovremennyye nauchnyye issledovaniya i innovatsii. 2020. № 1. [Elektronnyy resurs]. URL: https://web.snauka.ru/issues/2020/01/90380 (data obrashcheniya: 26.08.2025).
11. Krauze R. P. Issledovaniye metodicheskikh podkhodov k effektivnosti effektivnosti IT proyektov na predpriyatiyakh // Biznes-obrazovaniye v ekonomike znaniy. 2020. № 3. S. 87–92.
12. Shaburov A. S., Shlykov A. I. Razrabotka metoda otsenki ekonomicheskoy effektivnosti sistemy zashchity informatsii dlya kommercheskikh predpriyatiy // Vestnik PNIPU. Elektrotekhnika, informatsionnyye tekhnologii, sistemy upravleniya. 2020. № 36. S. 193–213.
13. Kurilo A. P., Parshin I. S., Simachkov S. A., Potapov G. D. Opredeleniye effektivnosti kompleksnykh sistem informatsionnoy bezopasnosti metodom ekspertnykh otsenok / Aktual'nyye problemy zashchity informatsii: sovremennost' i perspektivy. Materialy II Nauchno-prakticheskoy konferentsii. Moskva, 2025. S. 43–48.
14. Butusov I. V., Nashchekin P. A., Romanov A. A. Teoretiko-semanticheskiye aspekty organizatsii kompleksnoy sistemy zashchity informatsionnykh sistem // Voprosy kiberbez-opasnosti. 2016. № 1(14). S. 9–16.
15. Ziro A., Gnatyuk S., Toibayeva S. Investigation of the Method of Evaluating the Effectiveness of the Information Security System Based on Fuzzy Inference // Scientific Journal of Astana IT University. 2023. Volume 13. Pp. 52–63. DOI: 10.37943/13dzev3953.
16. Bratchenko A. I., Butusov I. V., Kobelyan A. M., Romanov A. A. Metody primeneniya teorii nechetkikh mnozhestv k snizheniyu riska vozniknoveniya vazhneyshikh svoystv zashchitnykh resursov upravlencheskikh sistem upravleniya // Voprosy kiberbezopasnosti. 2019. № 1(29). S. 18–24.
17. Yermakov S. A., Chursin A. G., Bolgov A. A. Nechetko-mnozhestvennaya metodika otsenki riska dorozhnoy sistemy «umnyy dom» s dinamicheskoy topologiyey // Informatsiya i bezopasnost'. 2022. T. 25. Vyp. 4. S. 495–500.
18. Wojtaszek H. et al. Methods for Assessing the Economic Efficiency of IT Projects // European research studies journal. 2024. Volume XXVII (Issue 3). Pp :637–651. DOI:10.35808/ersj/3457.
19. Kasim M. K. M. et al. A systematic literature review on the effect of information systems on the performance of government officials International // Journal of Advanced and Applied Sciences, 11(3) 2024, Pages: 46–54.
20. Ivanova L. N., Lugovskoy V. D. Ekspertnyye otsenki v upravlencheskikh resheniyakh // Sovremennyye nauchnyye issledovaniya i innovatsii. 2020. № 10 [Elektronnyy resurs]. URL: https://web.snauka.ru/issues/2020/10/93677 (data obrashcheniya: 26.08.2025).