СИСТЕМА ПОКАЗАТЕЛЕЙ КАЧЕСТВА СЕТЕОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ УСЛУГ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Карганов В. В.[1], Рябов Г. А.[2], Яровой Р. В.[3]

DOI:10.21681/3034-4050-2025-6-28-42

Ключевые слова: *моделирование процессов, безопасность информации, информационные системы, цифровые технологии, сетевые сервисы, защита данных, оценка защищенности, весовые коэффициенты, интегральный показатель, моделирование угроз, аудит безопасности, устойчивость, адаптивность, когерентность, конфиденциальность.*

Аннотация

Цель исследования *заключается в разработке и формализация совокупности показателей, способных отражать не только текущее состояние безопасности, но и устойчивость системы к нарастающим угрозам при сохранении критически важной функциональности.*

Методы исследования: *анализируется проблема неоднозначности подходов к выбору параметров оценки и предлагаются пути ее решения с помощью системного подхода, моделирования угроз и применения теоретико-множественных методов. В качестве основных методов исследования используются: анализ существующих стандартов и подходов к обеспечению информационной безопасности; разработка функциональных моделей оценки; построение математических выражений для определения степени соответствия заданным требованиям.*

В результате *предложена классификация показателей по уровням абстракции, а также обоснованы критерии их адаптации к специфике конкретного объекта информатизации. Итогом работы стало создание универсальной, но гибкой структуры оценочных параметров, применимой как в государственных, так и в коммерческих системах.*

Научная новизна *работы заключается в разработке иерархической архитектуры интегральных показателей, обеспечивающей переход от формального соответствия нормативным требованиям к управляемой, измеримой и адаптивной оценке реальной защищенности, а также в обосновании механизма агрегации частных индексов в обобщенный показатель с учетом приоритетов цифровой трансформации.*

Введение

Современное состояние цифрового пространства характеризуется глубокой интеграцией информационных технологий во все сферы жизни общества. В условиях сложившейся геополитической напряженности, когда киберпространство [1, с. 54] становится одной из ключевых арен стратегического противостояния, вопросы обеспечения информационной безопасности (ИБ) приобретают особую значимость. Увеличение масштабов взаимодействия между компонентами информационных систем (ИС), рост числа удаленных доступов, переход на облачные технологии, внедрение сквозных технологий и другие аспекты – всё это создает условия, в которых традиционные подходы к защите данных становятся недостаточно эффективными. На первый план выходит необходимость создания комплексной системы оценки, которая позволила бы не только фиксировать текущее состояние защищенности, но и прогнозировать возможные уязвимости в условиях динамично меняющейся среды.

Констатация вышеизложенного находит свое подтверждение и в ряде нормативно-правовых актах, руководящих документах Российской Федерации (РФ) по данному направлению исследования, в частности:

1 Карганов Виталий Вячеславович, кандидат технических наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: vitalik210277@mail.ru

2 Рябов Геннадий Анатольевич, старший научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт-Петербург, Россия. E-mail: grif999@mail.ru

3 Яровой Роберт Владимирович, научный сотрудник научно-исследовательского центра Военной академии связи, г. Санкт Петербург, Россия. E-mail: nadzar@yandex.ru

- концепция [2] глава III п. 15. п.п. 5 «развитие безопасного информационного пространства, защита российского общества от деструктивного иностранного информационно-психологического воздействия»; п. 30 п.п. 3 «обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети «Интернет» на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;
- реализация стратегического направления на основании распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р., предусматривающая достижение ряда показателей национальных целей развития РФ, определенных Указом Президента РФ от 21 июля 2020 г. № 474. Кроме того, приведены ряд проблемных задач, которые требуют их решения, в частности: «повышение уровня надежности и безопасности ИС, технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения (ПО), происходящих из иностранных государств»;
- распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р., глава III п. 1 «…нарушение безопасности инфраструктуры, продукции и производственных процессов, включая ИБ»;
- ГОСТ Р ИСО/МЭК 27004-2022, рекомендует использовать как количественные, так и качественные показатели (частота инцидентов, время реагирования, уровень уязвимостей). Согласно п. 4.1 «…измерения должны поддерживать постоянное улучшение системы менеджмента ИБ и помогать принимать обоснованные решения»;
- а также и другие РД, определяющие методологию измерения эффективности мер ИБ, включая показатели эффективности, метрики и индикаторы в области единого информационного пространства.

Принимая во внимание вышеизложенное, выбранное направление заявленной тематики, подразумевает необходимость мониторинга эффективности защиты системы, где рассматриваемые и предлагаемые показатели должны быть частью системы управления ИБ.

Целью исследования данной публикации является, разработка и обоснование системы показателей качества сетеориентированных информационных услуг (СИУ) ИБ, предназначенных для применения в процессе проектирования и эксплуатации объектов информатизации (ОИ). Основной задачей стало создание универсального, но гибкого механизма оценки, учитывающего специфику различных типов ИС и реагирующего на изменения внешней среды угроз.

В соответствии с этим, гипотеза исследования заключается в том, что применение методологических подходов позволит построить гибкую, измеримую и управляемую систему показателей качества ИБ для СИУ, обеспечивающую переход от формального соответствия к реальной защищенности, а также обеспечить прогнозируемое поведение системы в условиях внешних угроз.

1. Проблема оценки качества СИУ в области информационной безопасности

На сегодняшний день большинство подходов к оценке состояния ИБ ограничиваются проверкой наличия определенных компонентов: антивирусного ПО, систем контроля доступа и другие. Однако такой подход не позволяет судить о реальном уровне защищенности в условиях динамически изменяющейся среды угроз. Особенно остро эта проблема стоит для объектов, находящихся в зоне ответственности государственных структур, где последствия даже небольшой уязвимости могут быть катастрофическими.

Стоит акцентировать внимание на то, что безопасность одной системы не может рассматриваться изолированно, если она взаимодействует с десятками других, тем более, когда речь идет о государственном секторе, где каждая из имеющихся систем с своим предназначением может стать вектором проникновения. Здесь, необходим переход от парадигмы «оборонительных точек» к парадигме «устойчивых экосистем», когда оценивается не только наличие средств защиты, но и способность всей сети сохранять целостность, конфиденциальность и доступность даже при частичном компрометировании.

Ввиду этого отсутствие единых критериев оценки приводит к том, что одна и та же система может считаться защищенной по одним показателям и уязвимой по другим. Это создает ложное ощущение безопасности и снижает готовность к реальным угрозам. Также наблюдается недостаточная проработка

вопросов сетевой устойчивости: большинство стандартов и рекомендаций сосредоточены на внутреннем состоянии системы и не учитывают ее поведение в условиях сетевого взаимодействия.

Наряду с представленной проблематикой, а также ряда основополагающих паллиативных вопросов и задач, приведенных в РД, для последующего повествования материала, необходимо дать определения в части введенных терминов, которые в последующем будут использованы и применены с их параметрами для достижения поставленной цели исследования.

2. Определения терминов, используемых в данном исследовании

Как было упомянуто выше, для построения и обоснования корректной системы показателей необходимо привести лаконичные понятия, которые прежде всего регламентированы РД в данной предметной области, а также декомпозированы и детализированы на основании синопсиса апробированных материалов настоящей области исследования.

Качество – это степень соответствия совокупности присущих характеристик объекта требованиям[2].

Критерий качества – это набор параметров и показателей, используемых для оценки степени соответствия продукции, услуг или процессов установленным стандартам и требованиям[4].

Информационная безопасность – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются конституционные права граждан, суверенитет и территориальная целостность РФ, устойчивое развитие общества и государства[5].

Признак качества ИБ – это свойство или характеристика системы защиты информации (ЗИ), которая свидетельствует о наличии или отсутствии определенного уровня безопасности, но пока не выражена в количественной форме[4]. Вот некоторые признаки качества ИБ: конфиденциальность, целостность, доступность, точность, устойчивость и другие. Также в 2025 году к признакам качества ИБ относят способность систем динамически адаптироваться к угрозам и предоставлять оцифрованные доказательства защищенности. Стоит отметить, тот факт, что признак может в дальнейшем быть формализован в критерий или показатель.

Критерий качества ИБ – это измеримый показатель, по которому оценивается эффективность мер ЗИ, то есть насколько хорошо обеспечивается конфиденциальность, целостность и доступность данных в конкретной системе или процессе[4].

Показатель качества ИБ – количественная или качественная характеристика, отражающая степень достижения цели в области ИБ[4].

Интегральный показатель качества ИБ ($I_{\text{ПКИБ}}$) – это обобщенная метрика, формируемая на основе агрегации частных показателей и отражающая общее состояние защищенности системы. $I_{\text{ПКИБ}}$ служит основой для принятия управленческих решений[4].

Услуга по обеспечению ИБ – комплекс действий, направленных на обеспечение конфиденциальности, целостности и доступности информации[4].

Информационные услуги в области ИБ – это услуги, направленные на обеспечение ЗИ, включая консультирование, аудит, мониторинг, внедрение систем защиты, обучение персонала, реагирование на инциденты и другие действия, связанные с управлением рисками и обеспечением безопасности ИС[6].

Сетевая ориентированность – совокупность свойств системы, обеспечивающих ее функциональную устойчивость и защиту в условиях сетевого взаимодействия [3, 4].

Сетеориентированные информационные услуги (СИУ) – программное средство, предоставляющее доступ к сетевым ресурсам и предоставляющее информацию о различных сервисах и услугах [3, 4].

Сетеориентированные информационные услуги ИБ – это комплекс действий, направленных на обеспечение конфиденциальности, целостности и доступности информации, предоставляемой в условиях распределенной сетевой среды. Такие услуги разрабатываются с учетом специфики сетевого пространства и предполагают наличие механизмов защиты передаваемых данных, контроля доступа извне, мониторинга трафика и реагирования

4 ГОСТ Р ИСО 9001-2015 Национальный стандарт Российской Федерации. Системы менеджмента качества. Требования. М.: Стандартинформ. 2020.

5 Доктрина информационной безопасности Российской Федерации», утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 (в ред. от 21.07.2021).

6 ГОСТ Р ИСО/МЭК 27035-2021. Информационные технологии. Методология управления инцидентами информационной безопасности [Текст]. – Москва: Стандартинформ, 2021. – 38 с.

на инциденты, возникающие в процессе сетевого взаимодействия [3, 4].

Объект информатизации – информационная система, программно-технический комплекс или иной субъект цифровой инфраструктуры, предназначенный для автоматизированной обработки данных [3].

3. Методологические основы построения системы показателей

Для построения и дальнейшего применения разрабатываемой системы показателей предлагается использовать совокупность следующих подходов: системный, моделирование угроз, теоретико-множественный. Анализ ряда источников в данной предметной области исследования, позволило ниже представить, краткое пояснения каждому из них.

1. Системный подход рассматривает ИБ не как набор разрозненных мер, а как целостную, иерархически организованную систему, где каждый элемент: технологии, процессы, человеческий ресурс, данные играют свою роль [5]. Показатели качества в этом подходе строятся «сверху вниз»: от стратегических целей организации – к тактическим процессам – к операционным метрикам. Это позволяет не просто измерять (что-то и где-то), а видеть, как локальные показатели влияют на общую безопасность. Главное преимущество – взаимосвязанность и управляемость. Подход позволяет сразу увидеть, как это повлияет на «количество инцидентов из-за человеческого фактора», а затем – на «уровень зрелости ИБ» всей организации.
2. Моделирование угроз, основан на выявлении потенциальных источников рисков и оценке их влияния на уровень защищенности [6], другими словами, задает содержание. По своей сути, именно он обнародует содержательные, релевантные показатели, привязанные к конкретным уязвимостям и тактикам злоумышленников. Этот подход делает систему показателей гибкой и адаптивной, а именно если появляется новая угроза, то нам не нужно перестраивать всю систему по новой, достаточно обозначить эту угрозу в виде нового показателя и уже исследовать с учетом нового показателя. Как правило такого типа подход применяется, тогда, когда угрозы меняются намного быстрее, чем нормативные документы, а сейчас это достаточно актуально, с учетом развития и внедрения цифровых технологий.
3. Теоретико-множественный подход, применяется для формализации множества параметров и их взаимосвязей. Он задает полноту и формальную корректность, что по своей сути вводит математическую строгость в построение системы показателей [7]. Этот подход особенно важен для СИУ, где критически важно соответствие требованиям к защите при передаче данных (шифрование, электронная цифровая подпись, контроль целостности). Подход обеспечивает верифицируемость и юридическую обоснованность оценки.

Анализ каждого из представленных подходов, позволил сформировать кратко своего рода достоинства и недостатки по отношению к каждому, в частности: системный, дает структуру, но не гарантирует релевантность рискам; моделирование угроз дает содержание, но не обеспечивает формальную верификацию; теоретико-множественный дает полноту, но не отражает динамику угроз. Поэтому для достижения поставленной цели исследования, предлагается использовать все три подхода, где применение каждого из них позволит для системы: задать структуру, содержание угроз и проверить полноту предлагаемого ОИ.

4. Архитектура системы показателей качества и критериев СИУ

Разрабатываемая и предлагаемая система показателей строится вокруг трех базовых измерений [3–5]:

- устойчивость, отражает способность системы сохранять работоспособность при внешних воздействиях;
- адаптивность, оценивает способность системы перестраиваться в ответ на изменение угроз;
- когерентность, характеризует согласованность поведения компонентов системы.

Каждое из них включает набор количественных и качественных критериев, объединенных в иерархическую структуру.

Принимая во внимание данные (п. 3 публикации), для последующей детализации, необходим переход к системному подходу, при котором качество СИУ рассматривается как

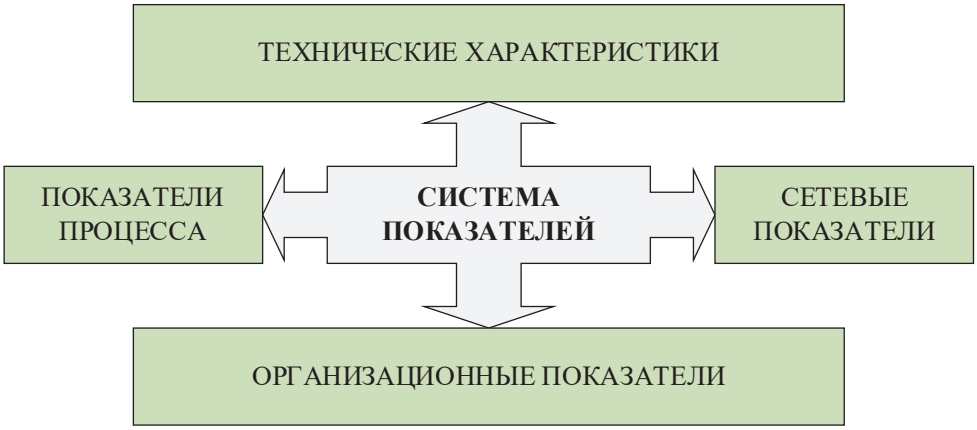


Рис. 1. Структура показателей качества (вариант)

синтез нескольких измерений, а затем подключить и другие подходы. Учитывая данный фактор, предлагается иерархическая система показателей, объединяющая технические, процессные, организационные и сетевые аспекты функционирования [3–6, 8, 9], так называемая четырехуровневая система показателей. Каждый уровень отражает специфические риски и ресурсы: от аппаратной защиты до устойчивости процедур реагирования на инциденты. Показатели формализованы, нормированы и интегрированы в общий индикатор качества, позволяющий сравнивать разнородные системы и прогнозировать их поведение при нагрузке.

Ввиду этого, для последующего представления иерархической системы показателей, предлагается обобщенная структура (рис. 1), которая показывает основополагающие ее составляющие.

Здесь стоит акцентировать внимание на том моменте, что для логической структуризации как ранее приведенного материала, так и его последующего повествования необходимо указать взаимосвязь с предлагаемой методологической основой построения системы показателей. Это придаст структурированности и логическому заключению рассматриваемого ОИ, в рамках достижения поставленной цели и как следствие подтверждения или опровержения гипотезы исследования.

В последующем детализация каждого отдельно взятого показателя рассматривается, как совокупность ряда его составляющих аспектов, которые придают целостность восприятия предлагаемого показателя.

1. Технические характеристики. Отражают физическую и программную реализацию защиты. Ориентированы на аппаратно-программные компоненты: серверы, маршрутизаторы, криптографические модули, средства контроля доступа [6; 10; 11, с. 179]. Его мысль заключается в измерении степени защищенности отдельных элементов системы с точки зрения их уязвимости перед известными и потенциальными угрозами. В качестве предполагаемых параметров можно принять: наличие и актуальность механизмов аутентификации и шифрования; уровень защищенности конфигурации; частота обновления микропрограмм и патчей; коэффициент технической уязвимости. Сфера применения: оценка готовности отдельных узлов к подключению сети, аудит перед развертыванием, мониторинг состояния оборудования. Представленные параметры по своему содержанию и их наполнению привязаны к подходу моделирования угроз, поскольку формируются на основе актуальных сценариев угроз.

2. Показатели процесса. Сосредоточены на процедурах, регламентах и циклах управления безопасностью. Отвечают за эффективность реализации политик в реальных условиях [11, с. 208; 12]. Здесь, его суть – это оценка зрелости процессов, от обнаружения инцидента до восстановления работоспособности. В роли его значений выступают: среднее время обнаружения угрозы; среднее время устранения; доля автоматизированных этапов в цепочке реагирования; периодичность проверки и актуализации планов восстановления. Особое внимание уделяется согласованности процессов по времени – например, совпадению моментов проведения аудита, резервного копирования и обновления политик. Несогласованность увеличивает количество

Таблица 1.

Взаимосвязь уровней к подходам и интегральным показателям

№ п/п	Уровень	Подход	Частный интегральный показатель
1	Организационный	Системный	Интегральный показатель системный (ИИПС)
2	Процессный	Системный	Интегральный показатель системный (ИИПС)
3	Технический	Моделирование угроз	Интегральный показатель угроз (ИИПУ)
4	Сетевой	Теоретико-множественный	Интегральный показатель полнота (ИИПП)

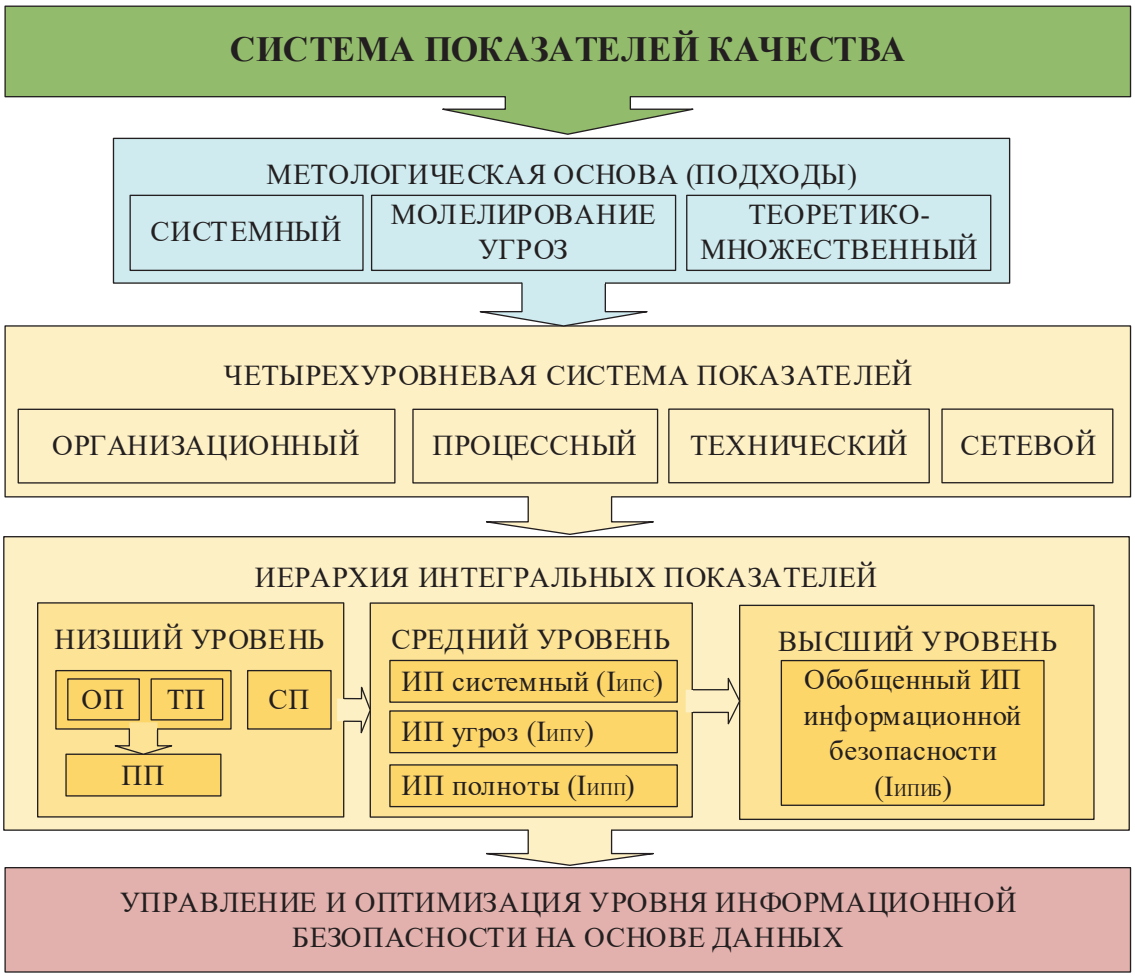
уязвимых мест. Применим он как: внутренний аудит, сертификация систем по стандартам ISO/IEC 27001:2022, оценка зрелости службы ИБ. Предлагаемые показатели, относятся к системному подходу, так как они есть ни что иное, как механизм, обеспечивающий работу системы ИБ.

3. Организационные показатели. Учитываются человеческий и институциональный факторы: распределение ролей, уровень подготовки персонала, культура безопасности [12; 13, с. 261]. Основополагающая идея заключается в измерении степени соответствия требований ИБ организационной среде. Для реализации необходимо рассматривать следующие данные по отношению к выше приведенной идеи: доля сотрудников, прошедших обучение по ИБ за последний год; количество назначенных ответственных за безопасность на уровне подразделений; уровень осведомленности, определяемый как отношение количества правильных ответов на тестовые сценарии к общему числу участников и ряд других не маловажных данных, которые отражены в источниках по данному направлению исследования. Область его применения, прежде всего зависит от его идеологии, в данном случае, это оценка готовности к внешним аудитам, анализ рисков при интеграции новых подразделений, управление кадровой политикой в сфере ИБ. В части их привязанности по отношению из ранее представленных подходов – системный, так как формирует основу для всех последующих мер.

4. Сетевые показатели. Особый класс, отражающий динамику и структуру взаимодействий между компонентами. В условиях сетеориентированных сервисов именно они определяют устойчивость к каскадным сбоям и скрытым атакам[7] [1; 6; 13, с. 258; 14, с. 121]. Концепция его применения, это оценка топологической и поведенческой устойчивости сети как целостной системы. В качестве входных данных можно использовать: степень централизации, определяемая через центральность по степени в графе связности; коэффициент избыточности маршрутов; время конвергенции сети после изменения топологии; мера доверительной согласованности – разброс в оценках доверия к одному узлу разными соседями. Высокая степень централизации увеличивает риски при компрометации центрального узла, в то время как избыточность маршрутов повышает отказоустойчивость. И как следствие, используются при: проектировании распределенных систем, мониторинга критически важных инфраструктур, моделирование сценариев отказов. Сетевые показатели привязаны к теоретико-множественному подходу, так как напрямую связан с формальным соответствием требованиям РД.

В результате, выше приведено описание четырехуровневой системы показателей качества. Здесь, каждый из четырех уровней дает частичное представление о ситуации. Систематика взаимосвязи между четырехуровневой системой показателей, предлагаемыми методологическими походами (см. п. 3) и как следствие интегральными показателями по отношению к каждому уровню системы, которые формируются на основании показателей уровней, позволили получить классификационную матрицу, результаты которой представлены в (табл. 1).

7 ГОСТ Р ИСО/МЭК 27004-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. М.: Стандартинформ. 50 с.



Примечание: *ОП – организационные показатели, ТП – технические показатели, ПП – процессные показатели, СП – сетевые показатели, ИП – интегральный показатель.*

Определение показателей зависит от задач, области и требований к системе.

Рис. 2. Иерархическая архитектура системы показателей качества

Проанализировав полученные данные (см. табл. 1), можно сформировать иерархическую структуру системы показателей качества СИУ в области ИБ, где предлагаемые методологические подходы обеспечивают основу для четырехуровневой детализации показателей. Схематично, данный результат представлен в виде графической иллюстрации (рис. 2).

Стоит отметить, что такого типа систематизация, позволит применить полученную систему показателей, как методику, которая может быть применена как универсальный инструмент для решения задачи оценки и управления уровнем ИБ.

Принимая во внимание, представленную выше иерархическую архитектуру, необходимо кратко пояснить механизм формирования интегральных показателей. При этом стоит уточнить ряд нюансов, в частности: числовые значения, которые будут упомянуты в последующем повествовании, были взяты на основании РД (ГОСТ Р ИСО/МЭК 27035-20214, ГОСТ Р ИСО/МЭК 27004-20215), и из практической области ранее апробированных материалов исследований данной предметной области[8] [13–18].

а) частный интегральный показатель системный (ИПС). Он формируется из показателей организационного и процессного уровней. С учетом проведенного анализа ряда материалов в данной предметной области исследования, для его расчета, используют в основном два наиболее приемлемые варианты, а именно:

8 Карганов, В. В. Эффективность сети связи на основе ее стратификации как сложной системы: Монография / В. В. Карганов, В. А. Кудряшов, А. Г. Расчесова – СПб.: ГНИИ «Нацразвитие», 2017. 128 с.

Вариант 1: $$I_{\text{ИПС}} = \frac{\sum(n_i \times k_i)}{\sum n_i} \times 100\ \%, \quad (1)$$

где: n_i – вес компонента, k_i – экспертная оценка i-го компонента по десяти бальной шкале. Другими словами, это подход в части качественной оценки.

Вариант 2: $$I_{\text{ИПС}} = \frac{(\text{К}_{\text{ОУ}} + \text{К}_{\text{ПУ}})}{2}, \quad (2)$$

где: $\text{К}_{\text{ОУ}}$ – количественный показатель организационного уровня, $\text{К}_{\text{ПУ}}$ – количественный показатель процессного уровня. Стоит отметить, что для данного расчета необходимо брать средние значения данных показателей, которые рассчитываются, как:

$$\text{К}_{\text{ОУ}} = \frac{\sum \text{К}_{\text{ОУ}}}{N}, \quad (3)$$

$$\text{К}_{\text{ПУ}} = \frac{\sum \text{К}_{\text{ПУ}}}{N}. \quad (4)$$

Здесь N – количество показателей.

б) частный интегральный показатель угроз ($I_{\text{ИПУ}}$), основа его – технические показатели уровня ($\text{К}_{\text{ТУ}}$). Позже мы вернемся к данному показателю, поскольку в последующем его формула расчета сыграет определенную роль в части получения ($I_{\text{ИПУ}}$).

Итак, для получения расчета ($I_{\text{ИПУ}}$), необходимо определиться с его компонентами.

Первый компонент – интегральный показатель времени реакции ($I_{\text{ИПР}}$), это промежуточный показатель, отражающий эффективность реагирования на инциденты:

$$I_{\text{ИПР}} = 100\ \% \times (1 - \frac{t_{\text{ср}}}{t_{\text{уст}}}), \quad (5)$$

где: $t_{\text{ср}}$ – среднее фактическое время реакции, $t_{\text{уст}}$ – установленное время.

Синопсис материалов исследований показал, что дополнительно может учитываться покрытие *MITRE ATT&CK* [19] – это второй компонент.

Покрытие *MITRE ATT&CK* – это оценка того, насколько хорошо текущая система безопасности охватывает актуальные техники и тактики, описанные в базе знаний *MITRE ATT&CK (Adversarial Tactics Techniques и Common Knowledge)*, которые обнаруживаются, предотвращаются или детектируются средствами защиты в системе.

Матрица *MITRE ATT&CK* используется для решения следующих задач:

- анализ существующей защиты на предмет соответствия реальным угрозам. Можно определить, к каким техникам уязвимы ресурсы организации, чтобы устранить критичные проблемы;
- своевременное реагирование на инциденты, где с помощью матриц можно установить, на каком этапе развития находится атака и какие меры необходимо принять в первую очередь;
- расследование киберинцидентов, здесь матрицы позволяют оперативно определить, на каком этапе обнаружена атака и где стоит в первую очередь искать следы вторжения.

Согласно [19] существует несколько способов оценки покрытия на базе знаний *MITRE*, но наиболее распространенные по: тактикам и техникам. В исследовании научной публикации наиболее приемлемо использовать расчет покрытия по техникам[9], это точнее отражает зрелость защиты:

$$O_{MITRE} = \frac{Q_{\text{тех}}}{Q_{\text{общ}}} \times 100\ \%, \quad (6)$$

где: O_{MITRE} – интегральный показатель технического уровня, отражающий готовность системы противостоять реальным сценариям атак; $Q_{\text{тех}}$ – количество покрытых техник; $Q_{\text{общ}}$ – общее количество техник.

С учетом полученных данных необходимо констатировать, что основополагающим показателем для ($I_{\text{ИПУ}}$) является технический показатель уровня ($\text{К}_{\text{ТУ}}$), который есть ни что иное, как среднее значение нормализованных показателей технического уровня:

$$\text{К}_{\text{ТУ}} = \frac{(I_{\text{ИПР}} + O_{MITRE})}{2}. \quad (7)$$

Систематизировав (5), (6), (7), а также руководствуясь РД и результатами практических апробаций данной предметной области исследования, следует:

$$I_{\text{ИПУ}} = \text{К}_{\text{ТУ}} \quad (8)$$

в) частный интегральный показатель полнота ($I_{\text{ИПП}}$). Здесь в качестве основы выступают сетевые показатели уровня ($\text{К}_{\text{СУ}}$), который в свою очередь рассчитывается по аналогии с ранее приведенными показателями согласно (3), (4), а именно:

$$\text{К}_{\text{СУ}} = \frac{\sum \text{К}_{\text{СУ}}}{N}. \quad (9)$$

Принимая во внимание (9), а также анализ ряда источников по данному направлению исследования, то для последующего получения (ИИПП), необходимо применить следующее:

9 Матрица Enterprise ATT&CK, 200 техник https://attack.mitre.org/

Таблица 2.

Данные для расчета интегральных показателей ИБ объекта исследования

№ п/п	Уровень	Показатель	Факт	Цель	Результат
1	Организационный	Процент сотрудников, прошедших обучение	80 %	100 %	80 %
2	Организационный	Наличие утвержденной политики ИБ	да	да	100 %
3	Процессный	Анализ рисков API [18] проводится	да	да	100 %
4	Процессный	Процент инцидентов, расследованных в срок	100 %	100 %	100 %
5	Технический	$t_{ср}$ реакции на инцидент	15 мин	≤60 мин	75 %*
6	Технический	Покрытие техник MITRE ATT&CK [19]	140	200	70 %
7	Сетевой	Процент передач с применением TLS и проверкой целостности	100 %	100 %	100 %
8	Сетевой	Наличие проверки целостности	да	да	100 %
9	Сетевой	Соответствие требованиям ФСТЭК	да	да	100 %

$$I_{\text{ИПП}} = \frac{P|D \cap F|}{P|F|} \times 100\ \%,$$

при условии

$$\frac{P|D \cap F|}{P|F|} = P\frac{D}{F} \qquad (10)$$

где: P – вероятность события; D – множество реализованных мер; F – множество требований РД.

Учитывая результаты исследований выявлено, что на практике сетевой уровень напрямую отражает соответствие требованиям РД, что также находит свое подтверждение и в ряду [12, 18, 20, с. 256]. В виду этого следует, что:

$$I_{\text{ИПП}} = \text{К}_{\text{СУ}}. \qquad (11)$$

Здесь $\text{К}_{\text{СУ}}$ – это среднее значение сетевых показателей.

г) обобщенный интегральный показатель ИБ ($I_{\text{ОИПИБ}}$). Проанализировав (2), (8), (11) и учитывая требования ISO/IEC 27004[10], ФСТЭК[11], выявлено что ключевыми драйверами эффективности ИБ признаются: управление рисками (40 %), реакция на угрозы (40 %), соответствие требованиям (20 %). Вследствие консолидации полученных результатов формула расчета ($I_{\text{ОИПИБ}}$) имеет вид:

$$I_{\text{ОИПИБ}} = 0{,}4 \times I_{\text{ИПС}} + 0{,}4 \times I_{\text{ИПУ}} + 0{,}2 \times I_{\text{ИПП}}. \qquad (12)$$

Принимая во внимание полученные данные, а также руководствуясь РД и результатами практических исследований, для апробации предлагаемых решений, ниже приведем пример оценки СИУ с применением выше представленных результатов. Полученные данные сведем в табличную форму, где в последующем это наглядно позволит нам удостовериться в эффективности применения разрабатываемой системы показателей.

5. Апробация предлагаемых решений

Для подтверждения и проверки полученных решений, а также определения оптимальных условий по реализации предлагаемых результатов, установленных в ходе научной публикации, воспользуемся таким объектом, как API-шлюз Единого портала государственных услуг. Поскольку, это одна из критически важных СИУ, обеспечивающая взаимодействие граждан, госорганов и ИС. Услуга использует стандартные протоколы защищенного взаимодействия: *OAuth 2.0* для аутентификации и TLS 1.2 (требования ФСТЭК[12], и РД[13]) для шифрования каналов передачи данных.

В процессе сбора данных путем непосредственного изучения, выбранного выше объекта, получены количественные значения каждого уровня: организационный, процессный, технический, сетевой. При этом в качестве показателей были использованы те, что наиболее часто рассматриваются по отношению к каждому уровню системы. Руководствуясь

10 ISO/IEC 27004:2023. Information security management – Monitoring, measurement, analysis and evaluation. – Geneva: ISO, 2023.

11 Методические рекомендации по формированию системы управления ИБ субъекта критической информационной инфраструктуры. ФСТЭК России. 2020. 48 с. https://fstec.ru/documents2/61726 (дата обращения 04.09.2025г).

12 Приказ ФСТЭК России от 11.02.2013 № 21 (ред. от 25.12.2020) «Об утверждении требований к защите информации...» // Официальный сайт ФСТЭК России. URL: https://fstec.ru (дата обращения: 03.09.2025).

13 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) // СПС «Гарант».

требованиями ФСТЭК[12], а также полученными формулами (см. п. 4 научной статьи) получены данные (табл. 2). Стоит отметить, что особое внимание уделено техническому уровню, где учтены как оперативность реагирования, так и полнота детектирования атак на основе базы знаний [19].

Из представленных результатов (см. табл. 2) необходимо привести некоторые пояснения в отношении их значений, в частности касательно технического уровня. Поскольку здесь учтены как оперативность реагирования, так и полнота детектирования атак на основе базы знаний *MITRE ATT&CK*.

Первый – это $t_{ср}$ реакции на инцидент (п. 5, табл. 2). Здесь в качестве $t_{уст}$ было принято значение 60 минут. Такой выбор значения обусловлен методическим рекомендациям ФСТЭК[12] и практике построения центров мониторинга безопасности[14] [21]. В частности, для некритических ИС допустимым считается время реагирования на инцидент до 1 часа, а целевое (оптимальное) время составляет 15 мин. и менее.

Второй, покрытие техник *MITRE ATT&CK* (п. 6, см. табл. 2). Данные для его расчета были взяты согласно матрице Enterprise ATT&CK[9] источника [19]. Здесь в качестве ($Q_{общ}$) было применено значение 200, поскольку именно оно, согласно матрице, является максимальным, в свою очередь значение ($Q_{тех}$) было основано на анализе практики по отношению к выбранному объекту в качестве примера, и составила 140.

Принимая во внимание выше полученные данные в ходе проведения исследования посредством настоящей научной публикации (см. табл. 2), а также выведенные формулы

14 Указ Президента Российской Федерации от 01.05.2022 г. № 250.

Таблица 3.

Результаты расчета интегральных и обобщенного интегрального показателей

№ п/п	Показатель	Формула	Расчет	Результат
1	$I_{ИПС}$	$I_{ИПС} = \frac{(К_{ОУ} + К_{ПУ})}{2}$	(90 + 100) / 2	95%
2	$К_{ОУ}$	$К_{ОУ} = \frac{\sum К_{ОУ}}{N}$	(80 + 100) / 2	90%
3	$К_{ПУ}$	$К_{ПУ} = \frac{\sum К_{ПУ}}{N}$	(100 + 100) / 2	100%
4	$I_{ИПР}$	$I_{ИПР} = 100\ \% \times (1 - \frac{t_{ср}}{t_{уст}})$	100 x (1 – 15 / 60)	75%
5	O_{MITRE}	$O_{MITRE} = \frac{Q_{тех}}{Q_{общ}} \times 100\ \%$	(140 / 200) x 100	70%
6	$К_{ТУ}$	$К_{ТУ} = \frac{(I_{ИПР} + O_{MITRE})}{2}$	(75 + 70) / 2	72,5%
7	$I_{ИПУ}$	$I_{ИПУ} = К_{ТУ}$	–	72,5%
8	$К_{СУ}$	$К_{СУ} = \frac{\sum К_{СУ}}{N}$	(100 + 100 + 100) / 3	100%
9	$I_{ИПП}$	$I_{ИПП} = К_{СУ}$	–	100%
	$I_{ОИПИБ}$	$I_{ОИПИБ} = 0{,}4 \times I_{ИПС} + 0{,}4 \times I_{ИПУ} + 0{,}2 \times I_{ИПП}$	0,4 x 95 + 0,4 x 72,5 + + 0,2 x 100	87%

для расчета частных интегральных показателей с их значениями, были полученные соответствующие результаты, которые сведены в таблицу 3. Для простоты понимания результата, в таблице также приведены как формулы, так и числовые значения.

Анализа полученных данных показал, что при имеющихся данных и непосредственно предлагаемой оценки системы показателей, ($I_{\text{ОИПИБ}}$) составил 87 % и в свою очередь оценивается как высокий. Наибольший вклад вносят системные процессы (95 %) и полное соответствие требованиям (100 %). Эффективность защиты от угроз (72,5 %) находится на хорошем уровне, что подтверждается как оперативным реагированием (75 %), так и достаточным охватом сценариев атак (70 % по O_{MITRE}).

Наряду с вышеизложенным, необходимо акцентировать внимание на том моменте, что согласно требованиям РД приведенными в контексте научной публикации, а также апробированным материалам в данной предметной области исследования, выявлены три ключевые интегральные показателя, а именно:

- время реакции системы на инциденты ИБ. Он дает количественную оценку состояния ИБ и позволяет судить о результативности принимаемых мер и средств управления и контроля;
- интегральная оценка качества защищенности ИС на основе экспертных оценок. Для этого каждый из экспертов независимо друг от друга оценивает качество защищенности системы по критериям от 0 до 1. Затем интегральная оценка вычисляется как среднее геометрическое этих оценок;
- интегральный показатель, характеризующий вероятность устойчивой работы и своевременного представления полной, достоверной и защищенной информации в системе информационной поддержки жизненного цикла сложных систем. Он определяется с учетом структуры системы, условий эксплуатации и предлагаемых проектных решений.

Проведенная их детализация, позволила установить, что они формулируются в разных источниках по-разному, но при этом достаточно устойчиво группируются вокруг трех основных идей: оперативность реагирования на инциденты; целостность управленческой и процессной основы; формальная и функциональная устойчивость при передаче информации.

Последующее сопоставление установленных выше интегральных показателей с методологическими подходами, позволило продемонстрировать не противоречие, а преемственность и систематизацию существующей практики. Полученные результаты, сведены в (табл. 4).

Анализируя полученные данные корреляции интегральных показателей (см. табл. 4) и учитывая ранее полученные результаты исследований научной публикации необходимо отметить по отношению к каждому приведенному показателю:

- первый показатель, измеряет скорость обнаружения и реагирования на реализованные угрозы. Показатель напрямую связан с эффективностью против реальных сценариев атак, что является ядром подхода моделирования угроз;
- второй показатель, отражает зрелость управленческих и технологических компонентов ИБ. Экспертная оценка охватывает структуру системы ИБ в целом – политики, процессы, роли, обучение, что соответствует системному подходу;
- третий показатель, характеризует надежность и соответствие требованиям при передаче данных в распределенных системах. Показатель формализован и проверяет соответствие множеству требований к доступности, целостности и конфиден-

Таблица 4.

Корреляция интегральных показателей с методологическими подходами

№ п/п	Интегральный показатель	Подход	Привязка
1	Время реакции на инциденты	Моделирование угроз	Формирует $I_{\text{ИПУ}}$
2	Экспертная оценка защищенности	Системный	Формирует $I_{\text{ИПС}}$
3	Вероятность устойчивой работы и защищенности информации	Теоретико-множественный	Формирует $I_{\text{ИПП}}$

циальности, что лежит в основе теоретико-множественного подхода.

Это свидетельствует о том, что три интегральных показателя (см. табл. 4) не противоречат предложенному решению научной публикации, а, напротив, естественным образом встраиваются в ее логическую структуру. И как следствие разработанная система показателей качества и критериев СИУ в области ИБ не отвергает существующую практику, а обобщает и систематизирует ее, придавая ей строгую методологическую основу и обеспечивая возможность объединения в единый интегральный показатель ИБ.

Заключение

Гипотеза исследования, согласно которой синтез методологических подходов, приведенных в научной публикации, позволяет построить гибкую, измеримую и управляемую систему показателей качества СИУ в области ИБ, подтверждена. В ходе работы были не только разработаны частные и обобщенные интегральные показатели на основе четырехуровневой структуры, но и обоснована их корреляция с тремя известными интегральными показателями, выявленными в научных источниках предметной области исследования:

- время реагирования на инциденты, где подход, основан на моделировании угроз;
- экспертная оценка защищенности – системный подход;
- вероятность устойчивой работы и защищенности информации, сопоставим с теоретико-множественным подходом.

Это свидетельствует о том, что предложенная система показателей не противоречит существующей практике, а обобщает, структурирует и формализует ее, обеспечивая переход от формального соответствия к реальной управляемости защищенностью.

Разработанная система показателей качества и критериев ИБ для СИУ обладает рядом ключевых преимуществ:

- гибкостью, возможностью адаптации к специфике ОИ;
- измеримостью, переходом от субъективных оценок к количественным показателям;
- управляемостью, возможностью прогнозирования влияния изменений на общий уровень ИБ;
- верифицируемостью, формальной проверкой соответствия требованиям нормативных документов.

В то же время следует учитывать, что ее применение требует первоначальных усилий по сбору и нормализации данных, а также может потребовать корректировки весовых коэффициентов в зависимости от профиля ОИ. Например, для критически важной информационной инфраструктуры приоритетным становится соответствие требованиям, что повышает значимость теоретико-множественного компонента. Именно такие адаптивные подходы, ориентированные на данные, становятся необходимыми в условиях стремительного развития цифровых технологий, где традиционные методы оценки уступают место системам непрерывного мониторинга и управления рисками.

Разработанная система показателей рекомендуется к применению при оценке ИБ сетеориентированных информационных сервисов, включая API-шлюзы, облачные платформы и распределенные микросервисные архитектуры. В рамках исследования был приведен пример расчета ІОИПИБ, его результат 87 %, свидетельствует о высоком, но не предельном уровне защищенности и указывает на резервы для улучшения – в частности, на необходимость расширения охвата сценариев атак по базе знаний MITRE ATT&CK.

Таким образом, предложенная система показателей качества СИУ в области ИБ соответствует стратегическим приоритетам цифровой трансформации, в рамках которой вопросы обеспечения безопасности становятся неотъемлемой частью жизненного цикла ИС. В условиях молниеносного развития технологий, включая широкое внедрение искусственного интеллекта и автоматизированных решений, именно измеримые и адаптивные подходы к оценке ИБ позволяют обеспечить устойчивость цифровой среды. Как отмечено в Доктрине ИБ РФ3, «повышение уровня защищенности информационных ресурсов достигается путем внедрения систем непрерывного мониторинга, оценки эффективности мер защиты и управления рисками на основе объективных критериев». Предложенная система показателей качества СИУ в области ИБ как раз и предоставляет такой инструментарий – основанный на данных, поддающийся проверке и ориентированный на реальные угрозы.

Литература

1. Карганов В. В. Глава 1. Основные понятия, общеметодологические принципы технологии защиты информации в условиях кибернетического противоборства / В. В. Карганов // В книге: Технологии защиты информации в условиях кибернетического противоборства. Костарев С. В., Карганов В. В., Липатников В. А. Санкт-Петербург, 2020. С. 29–67.
2. Концепция внешней политики Российской Федерации. Указ Президента Российской Федерации № Пр-229 от 31.04.2023.
3. Сетеориентированные сервисы https://timeweb.cloud/tutorials/microservices/servis-orientirovannaya-arhitektura-i-mikroservisy-raznica (дата обращения: 27.08.2025 г.).
4. Даник, О. Л. Цифровая трансформация взаимодействия государства и граждан: от традиционных сервисов к клиентоцентричной модели / О. Л. Даник, Н. В. Куриная. – Текст: непосредственный // Молодой ученый. – 2025. – № 37(588). – С. 169–175. – URL: https://moluch.ru/archive/588/128388/.
5. Черкашин А. К. Математические аспекты реализации метода анализа иерархий /А. К. Черкашин / Информационные и математические технологии в науке и управлении. 2020. 1(17). 2020. С. 5–24.
6. Карганов В. В. Методология безопасности информации в текущих информационных системах / В. В. Карганов // В сборнике: Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПб., 2020. С. 21–27.
7. Козлов М. Ю. Теоретико-множественные модели в оценке соответствия требований ИБ // Безопасность информационных технологий. – 2022. – № 3. – С. 12–20.
8. Епишкин И. И. Модель управления при реализации проектов цифровой трансформации // Конференциум Асоу: Сб. научн. трудов и материалов научно-практических конференций. 2021. Вып. 4.
9. Кройц Д. и др. Об эффективности обновления политик безопасности в программно-конфигурируемых сетях. Материалы Международной конференции по сетевым протоколам (ICNP) 2020, С. 1–12.
10. Иванов А. С. Методы оценки зрелости систем информационной безопасности в условиях цифровой трансформации // Вопросы кибербезопасности. – 2023. – № 4. – С. 22–31.
11. Васильева Т. Ю., Куприянов А.И. Мельников В. П. Информационная безопасность. М.: КноРус. 2023. 372 с. (С. 154–228).
12. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. М.: Лань. 2021. 64 с.
13. Щербаков А. Ю. Информационная безопасность / А. Ю. Щербаков. – М.: Юрайт, 2023. – 456 с. (С. 254–276).
14. Григорьев С. А. Управление рисками в сетеориентированных информационных системах / С. А. Григорьев. – М.: Горячая линия – Телеком, 2024. – 288 с. (С. 112–125).
15. Носов, М. И. Концептуальные подходы моделирования единого информационного пространства подсистем специального назначения / М. И. Носов, В. В. Карганов / Военная мысль. 2019. № 1. С. 102–128.
16. Гродзенский Я. С. Информационная безопасность. Уч. пособие. М.: РГ-Пресс.2024. 144с. (С.46–64).
17. Щербак А. В. Информационная безопасность. М.: Юрайт. 2023. 260с. (С.192–248)
18. Петров Д. В., Смирнова Е. А. Интегральные показатели эффективности защиты API в распределенных системах // Информационно-измерительные и управляющие системы. – 2024. – Т. 22, № 2. – С. 45–53.
19. MITRE ATT&CK Framework. – URL: https://attack.mitre.org (дата обращения: 10.09.2025).
20. Нестеров С. А. Основы информационной безопасности. М.: Лань. 2023.324с. (С. 221–264).
21. Проблемы SOC. https://rt-solar.ru/services/jsoc/blog/3471/?ysclid=mg5454ij5396963933 (дата обращения: 18.09.2025 г.)

SYSTEM OF QUALITY INDICATORS OF NETWORK-ORIENTED INFORMATION SERVICES IN THE FIELD OF INFORMATION SECURITY OF INFORMATIZATION OBJECTS

Karganov V. V.[15], Ryabov G. A.[16], Yarovoy R. V.[17]

15 Vitaly V. Karganov, Ph.D. of Technical Sciences, Associate Professor, Senior Researcher of the Research Center of the Military Academy of Communications, St. Petersburg, Russia. E-mail: vitalik210277@mail.ru

16 Gennady A. Ryabov, Senior Researcher, Research Center, Military Academy of Communications, St. Petersburg, Russia. E-mail: grif999@mail.ru

17 Robert V. Yarovoy, Researcher of the Research Center of the Military Academy of Communications, St. Petersburg, Russia. E mail: nadzar@yandex.ru

Keywords: *process modeling, information security, information systems, digital technologies, network services, data protection, security assessment, weight ratios, integral indicator, threat modeling, security audit, resilience, adaptability, coherence, confidentiality.*

Abstract

The purpose of the study *is to develop and formalize a set of indicators that can reflect not only the current state of security, but also the system's resilience to growing threats while maintaining critical functionality.*

Research methods: *the problem of ambiguity of approaches to the choice of assessment parameters is analyzed and ways to solve it are proposed using a systematic approach, threat modeling and the use of set-theoretic methods. The main research methods are: analysis of existing standards and approaches to ensuring information security; development of functional assessment models; construction of mathematical expressions to determine the degree of compliance specified requirements.*

As a result*, the classification of indicators by levels of abstraction is proposed, as well as the criteria for their adaptation to the specifics of a particular object of informatization are substantiated. The result of the work was the creation of a universal, but flexible structure of evaluation parameters applicable both in state and commercial systems.*

The scientific novelty *of the work lies in the development of a hierarchical architecture of integral indicators, which ensures the transition from formal compliance with regulatory requirements to a manageable, measurable and adaptive assessment of real security, as well as in the substantiation of the mechanism for aggregating private indices into a generalized indicator, taking into account the priorities of digital transformation.*

References

1. Karganov V. V. Glava 1. Osnovnye ponjatija, obshhemetodologicheskie principy tehnologii zashhity informacii v uslovijah kiberneticheskogo protivoborstva / V.V. Karganov // V knige: Tehnologii zashhity informacii v uslovijah kiberneticheskogo protivoborstva. Kostarev S. V., Karganov V. V., Lipatnikov V. A. Sankt-Peterburg, 2020. S. 29–67.
2. Koncepcija vneshnej politiki Rossijskoj Federacii. Ukaz Prezidenta Rossijskoj Federacii № Pr-229 ot 31.04.2023.
3. Seteorientirovannye servisy https://timeweb.cloud/tutorials/microservices/servis-orientirovannaya-arhitektura-i-mikroservisy-raznica (data obrashhenija: 27.08.2025 g.)
4. Danik, O. L. Cifrovaja transformacija vzaimodejstvija gosudarstva i grazhdan: ot tradicionnyh servisov k klientocentrichnoj modeli / O. L. Danik, N. V. Kurinaja. – Tekst: neposredstvennyj // Molodoj uchenyj. – 2025. – № 37(588). – S. 169–175. – URL: https://moluch.ru/archive/588/128388/.
5. Cherkashin A. K. Matematicheskie aspekty realizacii metoda analiza ierarhij /A. K. Cherkashin / Informacionnye i matematicheskie tehnologii v nauke i upravlenii. 2020. 1(17). 2020. S. 5–24.
6. Karganov V. V. Metodologija bezopasnosti informacii v tekushhih informacionnyh sistemah / V. V. Karganov // V sbornike: Nacional'naja bezopasnost' Rossii: aktual'nye aspekty. Sbornik izbrannyh statej Vserossijskoj nauchno-prakticheskoj konferencii. SPb., 2020. S. 21–27.
7. Kozlov M. Ju. Teoretiko-mnozhestvennye modeli v ocenke sootvetstvija trebovanij IB // Bezopasnost' informacionnyh tehnologij. – 2022. – № 3. – S. 12–20.
8. Epishkin I. I. Model' upravlenija pri realizacii proektov cifrovoj transformacii // Konferencium Asou: Sb. nauchn. trudov i materialov nauchno-prakticheskih konferencij. 2021. Vyp. 4.
9. Krojc D. i dr. Ob jeffektivnosti obnovlenija politik bezopasnosti v programmno-konfiguriruemyh setjah. Materialy Mezhdunarodnoj konferencii po setevym protokolam (ICNP) 2020, S. 1–12.
10. Ivanov A. S. Metody ocenki zrelosti sistem informacionnoj bezopasnosti v uslovijah cifrovoj transformacii // Voprosy kiberbezopasnosti. – 2023. – № 4. – S. 22–31.
11. Vasil'eva T. Ju., Kuprijanov A. I. Mel'nikov V.P. Informacionnaja bezopasnost'. M.: KnoRus. 2023. 372 s. (S. 154–228).
12. Galygina L. V., Galygina I. V. Social'nye aspekty informacionnoj bezopasnosti. Laboratornyj praktikum. M.: Lan'. 2021. 64 s.
13. Shherbakov A. Ju. Informacionnaja bezopasnost' / A. Ju. Shherbakov. – M.: Jurajt, 2023. – 456 s. (S. 254–276).
14. Grigor'ev S. A. Upravlenie riskami v seteorientirovannyh informacionnyh sistemah / S. A. Grigor'ev. – M.: Gorjachaja linija-Telekom, 2024. – 288 s. (S. 112–125).
15. Nosov, M. I. Konceptual'nye podhody modelirovanija edinogo informacionnogo prostranstva podsistem special'nogo naznachenija / M. I. Nosov, V. V. Karganov / Voennaja mysl'. 2019.№ 1. S. 102–128.

16. Grodzenskij Ja. S. Informacionnaja bezopasnost'. Uch. posobie. M.: RG-Press.2024. 144 s. (S. 46–64).
17. Shherbak A. V. Informacionnaja bezopasnost'. M.: Jurajt. 2023. 260s. (S.192–248)
18. Petrov D. V., Smirnova E. A. Integral'nye pokazateli jeffektivnosti zashhity API v raspredelennyh sistemah // Informacionno-izmeritel'nye i upravljajushhie sistemy. – 2024. – T. 22, № 2. – S. 45–53.
19. MITRE ATT&CK Framework. – URL: https://attack.mitre.org (data obrashhenija: 10.09.2025).
20. Nesterov S. A. Osnovy informacionnoj bezopasnosti. M.:Lan'. 2023.324s. (S. 221–-264).
21. Problemy SOC https://rt-solar.ru/services/jsoc/blog/3471/?ysclid=mg5454ij5396963933 (data obrashhenija: 18.09.2025 g.)