19. *Chastikova V.A., Bakhtin A.S., Merkulov P.A.* Razrabotka metodiki integratsii bol'shikh yazykovykh modeley v protsessy tsentra monitoringa informatsionnoy bezopasnosti [Development of a methodology for integrating large language models into the processes of an information security monitoring center], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2025, No. 4 (246), pp. 57-69.
20. *Martino A., Iannelli M., Truong C.* Knowledge injection to counter large language model (LLM) hallucination, *European Semantic Web Conference*. Cham: Springer Nature Switzerland, 2023, pp. 182-185.
21. *Ye H.* et al. Ontology-enhanced Prompt-tuning for Few-shot Learning, *Proceedings of the ACM Web Conference 2022*, 2022, pp. 778-787.
22. *Goyal S., Doddapaneni S., Khapra M.M., Ravindran B.* A Survey of Adversarial Defences and Robustness in NLP, *arXiv.org*, 2023, 43 p. Available at: https://doi.org/10.48550/arXiv.2203.06414.
23. *Sharma R.K., Gupta V., Grossman D.* SPML: A DSL for Defending Language Models Against Prompt Attacks School of Computer Science & Engineering, *arXiv.org*, 2024. Available at: https://doi.org/10.48550/arXiv.2402.11755.
24. *Yu Z., Liu X., Liang S., Cameron Z., Xiao C., Zhang N.* Don't listen to me: understanding and exploring jailbreak prompts of large language models, *arXiv.org*, 2024. Available at: https://doi.org/10.48550/arXiv.2403.17336.
25. OpenAI Guardrails: zashchita II-prilozheniy ot atak [OpenAI Guardrails: Protecting AI Applications from Attacks]. Available at: https://habr.com/ru/articles/968516/ (accessed 20 April 2026).
26. *Li Z., Ning H.* Autonomous GIS: The next-generation AI-powered GIS, *International Journal of Digital Earth*, 2023, Vol. 16, No. 2, pp. 4668-4686. DOI: 10.1080/17538947.2023.2278895.
27. *Hahsler M., Piekenbrock M., Doran D.* dbscan: Fast Density-Based Clustering with R, *Journal of Statistical Software*, 2019, Vol. 91, No. 1. DOI: 10.18637/jss.v091.i01.

Беляков Станислав Леонидович – Южный федеральный университет; e-mail: sbelyakov@sfedu.ru; г. Таганрог, Россия; кафедра информационно-аналитических систем безопасности; д.т.н.; профессор.

Израилев Лев Алексеевич – Южный федеральный университет; e-mail: izrailev@sfedu.ru; г. Таганрог, Россия; тел.: +79185608305; кафедра информационно-аналитических систем безопасности; аспирант.

Покусаев Олег Николаевич – Российский университет транспорта (МИИТ); e-mail: o.pokusaev@rut.digital; г. Москва, Россия; проректор; к.э.н.; доцент.

Belyakov Stanislav Leonidovich – Southern Federal University; e-mail: sbelyakov@sfedu.ru; Taganrog, Russia; the Department of Information Analytical Systems of Safety; dr. of eng. sc.; professor.

Izrailev Lev Alekseevich – Southern Federal University; e-mail: izrailev@sfedu.ru; Taganrog, Russia; the Department of Information Analytical Systems of Safety; phone: +79185608305; postgraduate student.

Pokusaev Oleg Nikolaevich – Russian University of Transport (MIIT); e-mail: o.pokusaev@rut.digital; Moscow, Russia; Vice-rector; cand. of ec. sc.; associate professor.

УДК 004.056.5:343.148.6 DOI 10.18522/2311-3103-2026-3-45-68

Е.С. Абрамов

МЕТОДОЛОГИЯ ВЫЧИСЛИТЕЛЬНОЙ ФОРЕНЗИКИ И ФОРМАЛЬНАЯ ВЕРИФИКАЦИЯ ЭКСПЕРТНЫХ ВЫВОДОВ

Рассматривается фундаментальная проблема преодоления системного гносеологического кризиса в судебной компьютерно-технической экспертизе. Данный кризис вызван нарастающим смысловым (семантическим) разрывом между вероятностной, стохастической природой цифровых следов, подверженных влиянию анти-форензики, и строгими требованиями состязательного правосудия к юридической определённости доказательств. Настоящая статья носит концептуальный характер и закладывает теоретический базис вычислительной форензики как самостоятельной научной дисциплины. В работе обосновывается необходимость смены парадигмы: от традиционного эвристического поиска артефактов и субъективного мнения эксперта к методологии, опирающейся на принципы алгоритмической воспроизводимости, измеримости неопределённости и формальной верифицируемости. Автором разработана теоретико-множественная онтологическая модель компьютерного инцидента, базирующаяся на триаде «субъект – способ – объект» (S-M-O) и аксиоме сохранения следа процесса. Эта модель позволяет взаимно-однозначно проецировать технические индикаторы (IoA, IoB, IoC) на юридические признаки состава преступления. Предложена методология формальной проверки истинности гипотез, включающая критерии структурной полноты, причинно-следственной связности, непротиворечивости и фактической обоснованности. Впервые в научный оборот введена математическая модель оценки достоверности экспертного вывода с использованием логистической функции (функции доверия). Данная

модель позволяет рассчитать вероятность юридически значимого факта путём агрегации метрик таксономического соответствия, силы каузальных связей на графе инцидента и штрафа за энтропию среды. Применение разработанного подхода трансформирует реконструкцию инцидента из обратной некорректной задачи в детерминированную процедуру, обеспечивая математически доказуемую объективность доказательной базы даже в условиях неполноты данных и активного противодействия расследованию.

Вычислительная криминалистика; судебная экспертиза; компьютерный инцидент; формальная верификация; онтологическое моделирование; причинность; достоверность; энтропия.

E.S. Abramov

COMPUTATIONAL FORENSICS METHODOLOGY AND FORMAL VERIFICATION OF EXPERT FINDINGS

This paper addresses the fundamental challenge of overcoming the systemic epistemological crisis in digital forensics. This crisis is driven by an expanding semantic gap between the probabilistic and stochastic nature of digital traces—frequently compromised by anti-forensic techniques—and the rigorous demands of adversarial legal proceedings for the legal certainty of evidence. The article is conceptual in nature and establishes the theoretical foundation of computational forensics as an independent scientific discipline. The study justifies a necessary paradigm shift from traditional heuristic artifact-discovery approaches and subjective expert opinions toward a rigorous methodology grounded in the principles of algorithmic reproducibility, the measurability of uncertainty, and formal verifiability. The author develops a set-theoretic ontological model of a computer incident, which is built upon the "subject–method–object" (S-M-O) triad and the axiom of process trace conservation. This model enables a one-to-one mapping of low-level technical indicators (IoA, IoB, IoC) onto the legal elements of a crime (corpus delicti). Furthermore, a methodology for the formal verification of hypothesis validity is proposed, incorporating the criteria of structural completeness, causal coherence, logical consistency, and factual grounding. For the first time, a mathematical model for assessing the reliability of expert findings using a logistic function (trust function) is introduced into scientific discourse. This model enables the calculation of the probability of a juridical fact by aggregating taxonomic compliance metrics, the strength of causal relationships within the incident graph, and an environmental entropy penalty. The application of the developed approach transforms forensic incident reconstruction from an ill-posed inverse problem into a deterministic procedure, ensuring the mathematically provable objectivity of the evidentiary base even under conditions of incomplete data and active anti-forensic countermeasures.

Computational forensics; digital forensics; computer incident; formal verification; ontological modeling; causality; reliability; entropy.

1. Введение. Современный этап развития информационного общества характеризуется не только тотальной цифровизацией всех сфер деятельности, но и существенным изменением структуры преступности. Согласно официальным статистическим данным Министерства внутренних дел Российской Федерации, количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, демонстрирует устойчивую тенденцию к росту, составляя значительную долю в общей структуре криминальных деяний[1]. Одновременно с этим усложняются тактики, техники и процедуры (TTPs) злоумышленников: в отчётах ведущих центров мониторинга безопасности отмечается массовый переход к тактикам «жизни на земле» (Living off the Land, LoTL) и использованию инструментов анти-форензики, направленных на целенаправленное уничтожение цифровых следов[2]. В этих условиях традиционная судебная компьютерно-техническая экспертиза (СКТЭ) переживает системный гносеологический кризис.

Фундаментальная проблема заключается в нарастающем разрыве между возможностями классических криминалистических методик и реалиями современной киберпреступности. Если ранее исследователи били тревогу преимущественно из-за экспоненциального роста объёмов данных (так называемый «предел масштабируемости»), то в современных условиях, как показывают исследования Н. Сунде и Г. Хорсмана [1], кризис усугубляется многократно возросшей алгоритмической сложностью инцидентов. В то время как традиционные подхо-

[1] Состояние преступности в России за январь–декабрь 2024 года // Министерство внутренних дел Российской Федерации, 2025. – URL: https://мвд.рф/reports/item/46247385/.

[2] Развитие угроз в 2024 году. Статистика и тенденции // Securelist. – 2025. – URL: https://securelist.ru/it-threat-evolution-2024-statistics/108422/.

ды пытаются решить эту проблему экстенсивным путём (наращиванием вычислительных мощностей для ручного или эвристического поиска улик), наш анализ показывает, что данный путь достиг предела эффективности. Как подтверждает масштабный анализ С.Дж. Хуссейна [2], современный инструментарий характеризуется высокой фрагментацией: средства анализа облачных сред, мобильных устройств и классических носителей функционируют изолированно. Это делает невозможным построение сквозной причинно-следственной связи без единой теоретической надстройки.

Отечественная школа криминалистики заложила прочный концептуальный фундамент для осмысления этой проблемы. В фундаментальном труде В.А. Мещерякова [3] раскрыты теоретические основы механизма следообразования в специфической искусственной среде киберпространства. Как убедительно показывает автор, цифровой след представляет собой лишь изменение состояния вычислительной системы, которое изначально лишено правовой семантики и подвержено высокой энтропии. Опираясь на эту специфику, А.А. Бессонов [4] обосновывает острую необходимость полного отказа от устаревших методик в пользу построения «цифровых криминалистических моделей преступления».

Именно здесь возникает ключевое противоречие, требующее научного разрешения: конфликт между стохастической, фрагментированной природой цифровых следов и императивным требованием состязательного процесса к детерминированности юридического факта. Судебная система требует от эксперта категорических ответов («да/нет»), не допускающих неоднозначного толкования [5].

Ситуация усугубляется отсутствием в современной теории формализованных метрик, позволяющих численно оценить достоверность выводов. Существующие методы визуализации и графового анализа отлично справляются с моделированием угроз, однако в условиях отсутствия математически обоснованного критерия истины ретроспективная оценка качества заключения зачастую подменяется субъективной категорией «внутреннего убеждения» эксперта. Учитывая, что цифровой след лишён изначальной семантики, мы выдвигаем тезис о том, что реконструкция инцидента является обратной некорректной задачей, для решения которой субъективного опыта эксперта недостаточно.

Таким образом, актуальность исследования обусловлена необходимостью смены парадигмы: от эмпирического описания цифровых артефактов к их строгому математическому моделированию на основе триады "Субъект – Способ – Объект". Задачей настоящего исследования является разработка теоретических основ и методологического базиса формальной верификации в задачах вычислительной форензики, позволяющего перейти от вероятностных оценок к математически доказанной корректности реконструкции инцидента, обеспечивая тем самым юридическую значимость экспертного вывода в условиях неопределённости.

Настоящая работа является первой в серии публикаций, посвящённых построению целостной теории вычислительной форензики. В ней закладывается методологический фундамент и математический аппарат формальной верификации. Экспериментальная валидация и калибровка параметров модели на реальных инцидентах составляют предмет дальнейших исследований.

2. Обзор существующих подходов. Анализ современного состояния исследований в области компьютерно-технической экспертизы и защиты информации позволяет выделить три основных направления, эволюция которых привела к необходимости формирования новой методологии.

2.1. Становление и ограничения классической вычислительной форензики. Фундаментальный вклад в становление вычислительной форензики (Computational Forensics, CF) как самостоятельной научной дисциплины внесли работы К. Франке и С. Шрихари [6]. В своём программном труде авторы определили CF как применение количественных методов и алгоритмов для анализа криминалистических данных, сместив фокус с качественных экспертных оценок на математическое моделирование. Однако, как показывает новейший систематический обзор Т. Арифа (2025), классический подход CF сегодня сталкивается с пределом эффективности из-за беспрецедентного усложнения сетевых угроз [7].

Критический анализ наследия школы Франке выявляет существенное ограничение: историческая ориентация преимущественно на задачи распознавания в физическом мире (анализ почерка, дактилоскопия, обработка изображений). Предложенные методы эффективно решают задачу идентификации объекта («что это?»), но, как отмечают современные

исследователи, практически не затрагивают уровень семантической интерпретации событий («почему это произошло?» и «каков умысел?»). В контексте расследования киберинцидентов это порождает глубокий «семантический разрыв»: алгоритмы способны выявить аномалию на синтаксическом уровне, но не способны квалифицировать её как элемент состава преступления на уровне прагматики.

Попытки преодолеть это ограничение через интеграцию вычислительного интеллекта и методов Big Data привели к созданию мощных инструментов обнаружения следов в распределённых инфраструктурах [8]. Тем не менее, как подчёркивается в масштабном обзоре М. Амроллахи [9], повсеместное внедрение машинного обучения (ML) породило новую фундаментальную проблему – проблему «чёрного ящика».

Научная дискуссия последних лет (2024–2025 гг.) фокусируется на юридической ничтожности результатов, лишённых свойства интерпретируемости. В работе Й. Каврестада убедительно доказано, что отсутствие прозрачности алгоритмических решений является главным барьером для их признания в качестве судебных доказательств [10]. Ситуация критически обостряется с внедрением больших языковых моделей (LLM). Исследования Ф. Брейтингера по анализу дампов памяти с помощью LLM демонстрируют риск генерации ложных артефактов («галлюцинаций»), что противоречит требованиям к допустимости доказательств [11]. Данный тезис находит подтверждение в фундаментальном обзоре С. Риццо, где отсутствие методов объяснимого искусственного интеллекта (Explainable AI, XAI) классифицируется как основной фактор уязвимости экспертных заключений при их оспаривании в суде [12].

Таким образом, мы утверждаем, что текущий State-of-the-Art в вычислительной форензике характеризуется критическим противоречием: наличие мощных средств обнаружения при полном отсутствии формальных механизмов верификации и семантического связывания технических паттернов с правовыми категориями. Предлагаемый в данной работе онтологический подход направлен на решение именно этой задачи через введение математически доказуемой модели каузальной связности инцидента.

2.2. Состояние исследований в области математических моделей оценки достоверности. Проведённый анализ российских и зарубежных публикаций по тематикам «вычислительная форензика», «математическая модель оценки достоверности экспертных выводов», «количественная оценка доказательственной силы» и «вероятностные методы в судебной экспертизе» показал, что на сегодняшний день они представлены в научной литературе фрагментарно. Основной массив работ сосредоточен на правовых и организационных аспектах судебной экспертизы; исследования, содержащие формальную математическую постановку задач верификации цифровых доказательств или строгие количественные метрики достоверности, практически отсутствуют. Можно отметить работу [13], в которой рассматриваются различные теории, лежащие в основе классификации выводов эксперта и подходов к определению вероятности в экспертной практике и приводится валидация байесовского подхода к оценке достоверности выводов экспертизы. Однако авторы [13] предлагают комплексного аппарата для связи техники и доказательственной силы.

В российской научной периодике не обнаружено публикаций, предлагающих формализованные методы оценки достоверности экспертных выводов с использованием вероятностных моделей, логистической регрессии или иного аппарата, способного связывать технические индикаторы с мерой юридической доказательственной силы. В работе коллектива авторов [14] исследуется достоверность результатов СКТЭ различных типов компьютерных преступлений, получаемых с помощью методов искусственного интеллекта и машинного обучения. Авторы делают вывод о том, что на данный момент к возможностям указанных методов относятся некритически, а главной проблемой является отсутствие верифицированных методов и средств объективной оценки как самого мат. Аппарата, так и результатов его применения.

Аналогичная картина наблюдается и при анализе зарубежных источников: несмотря на существенный прогресс в области онтологического моделирования и автоматизированного обнаружения инцидентов, формальный инструментарий для численной оценки достоверности и автоматической верификации экспертных гипотез остаётся неразработанным. В отличие от отечественной научной литературы, в зарубежных публикациях проблематика количественной оценки доказательственной силы представлена значительно шире. Однако анализ этих работ показывает, что они, как правило, не предлагают целостной методологии формальной верификации экспертных выводов применительно к компьютерным преступлениям.

Можно выделить несколько ключевых направлений. Во-первых, это доминирующая в настоящее время парадигма отношения правдоподобия, которая признана международным стандартом логически корректной интерпретации веса отдельных улик [15, 16]. Во-вторых, активно развиваются методы формальной верификации, где предпринимаются попытки строгого доказательства наличия или отсутствия определённых событий в цифровой системе [17, 18]. В-третьих, существуют работы по байесовским сетям, которые позволяют моделировать сложные взаимосвязи между доказательствами.

Несмотря на значительный прогресс в каждой из этих областей, в литературе сохраняется принципиальный пробел. Работы, основанные на LR, ориентированы на оценку доказательственного веса отдельных артефактов и не предлагают механизма верификации всей гипотетической модели инцидента. Формальные методы, в свою очередь, фокусируются на технической реконструкции событий, оставляя за скобками их проекцию на юридический состав преступления – то есть не решают проблему «семантического разрыва», которая является центральной для судебной экспертизы.

Таким образом, синтез математического аппарата количественной оценки доказательств с формальными методами верификации и онтологическими моделями, связывающими технику и право, остаётся нерешённой задачей. Выявленный пробел подтверждает своевременность и оригинальность настоящего исследования, направленного на создание методологии формальной верификации и математического аппарата оценки достоверности в вычислительной форензике.

2.3. Онтологическое моделирование и семантический разрыв. Осознание проблемы «семантического разрыва» между техническими данными и их юридической интерпретацией привело к активному развитию онтологических подходов. Если в ранних работах усилия исследователей были сосредоточены на базовой стандартизации понятийного аппарата, то в современном научном дискурсе акцент сместился на критический анализ применимости этих моделей в автоматизированных системах. В частности, в системном обзоре М. Моргенштерна [19] подчёркивается, что, несмотря на обилие разработок, онтологии в сфере форензики остаются крайне фрагментированными, что препятствует их использованию для сквозной верификации в трансграничных расследованиях. Данный тезис находит развитие в работе Т. Силвы [20], где автор указывает на фундаментальный недостаток большинства существующих моделей: они носят статичный характер и успешно описывают структуру объектов, но не способны моделировать динамику развития инцидента и причинно-следственные связи в условиях высокой энтропии среды.

Параллельно развиваются методы обеспечения прослеживаемости (traceability) цифровых доказательств. На смену обобщённым фреймворкам прошлого десятилетия приходят решения, базирующиеся на технологиях распределённого реестра. Так, С. Ли предлагает использовать блокчейн-платформы для обеспечения неизменности цепочки владения (chain of custody), что позволяет технически гарантировать целостность данных на протяжении всего жизненного цикла расследования [21].

Однако, сталкивая эти подходы с задачами судебной экспертизы, мы констатируем, что они носят преимущественно описательный или инфраструктурный характер. В отличие от работ [19] и [21], предлагаемая нами методология направлена на преодоление этой «пассивности» онтологических моделей. Мы утверждаем, что простого структурирования знаний и обеспечения их неизменности недостаточно для формирования доказательной базы. В противовес существующим подходам, наше исследование предлагает математический аппарат для автоматической верификации истинности и непротиворечивости связей между элементами онтологии. Это позволяет перейти от регистрации фактов к доказательству «Цифровой истины» через вычисление силы причинных связей, что детально описывается в последующих разделах работы.

2.4. Метрики безопасности и оценка достоверности. Значительный вклад в развитие количественных оценок защищённости и методов моделирования угроз внесла отечественная научная школа И. В. Котенко. В современных исследованиях [22] предложены методики оценки защищённости на основе графов атак с использованием баз знаний NVD и MITRE ATT&CK, что позволяет объективизировать расчёт метрик безопасности для сложных гетерогенных инфраструктур. Проблематика визуализации этих метрик для обеспечения ситуационной осведомлённости эксперта находит развитие в работах [23], где предлагаются методы ин-

терактивного визуального анализа инцидентов. Тем не менее, как отмечается в критическом обзоре [24], существующие синтаксические модели графов и деревьев атак часто ограничены в способности передавать глубокую семантику инцидента, что затрудняет их использование в качестве прямого доказательства без дополнительной формализации.

Теоретический базис для анализа связности в таких структурах существенно дополняют исследования графов зависимостей. Согласно анализу [25], использование данных моделей позволяет математически обосновать устойчивость сети и выявить критические пути компрометации. Однако мы констатируем наличие фундаментального методологического разрыва: в то время как современные подходы [22] и [25] ориентированы преимущественно на оценку рисков и прогнозирование векторов атак (*Ex-Ante*), задачи судебной экспертизы требуют ретроспективного доказательства причинности (*Ex-Post*), что диктует необходимость адаптации этого математического аппарата под цели реконструкции.

Вместе с тем, анализ актуальных правовых и этических вызовов, представленный в работе [26], показывает, что в задачах судопроизводства метрик «риска» недостаточно – требуются объективные метрики «доказательной силы». Существующие модели представления доказательств, подробно разобранные [27], хотя и фокусируются на логике реконструкции событий, не решают задачу формальной верификации экспертного вывода. Мы утверждаем, что для обеспечения юридической значимости необходимо не просто последовательное описание действий, а математическое подтверждение того, что реконструированная картина инцидента является единственно возможной и непротиворечивой при заданном наборе следов. На устранение этого дефицита доказательности направлена предлагаемая в настоящей статье методология верификации на основе онтологической модели и функционала регуляризации.

3. Концептуальные основы вычислительной форензики. ***3.1. Авторское определение и предметная область.*** Преодоление выявленных в ходе анализа литературы противоречий требует фундаментального пересмотра онтологического статуса используемых методов. В рамках настоящего исследования мы подходим к вычислительной форензике (Computational Forensics) не как к прикладному набору утилит, а как к фундаментальной научной дисциплине.

Базируясь на системном анализе проблемной области, сформулируем авторское определение:

Вычислительная форензика – это научная дисциплина, изучающая методы количественного моделирования процессов возникновения, видоизменения и фиксации цифровых следов с целью преобразования стохастических данных первичных измерений в детерминированные, математически верифицируемые доказательные факты в контексте задачи формальной верификации.

Данное определение фиксирует необходимый сдвиг парадигмы доказывания: переход от экспертного (нарративного) подхода, базирующегося на субъективном опыте интерпретатора, к формальному подходу, основанному на математических моделях и алгоритмической верификации. В новой парадигме цифровое доказательство должно представлять собой не «правдоподобное объяснение» событий, а строго «верифицируемый вывод», полученный в результате вычислений.

Предметная область CF существенно расширяет границы традиционной компьютерно-технической экспертизы (КТЭ). Если классическая КТЭ фокусируется на феноменологии инцидента, отвечая на вопросы «Что произошло?», «Где находятся данные?» и «Когда случилось событие?», то вычислительная форензика переносит фокус на онтологию и эпистемологию инцидента. Ключевыми вопросами здесь становятся:

- «С какой вероятностью наблюдаемые следы соответствуют выдвинутой гипотезе?».
- «Насколько достоверно полученное значение?».
- «Какова сила причинно-следственной связи (*causality, каузальность*) между действием и последствием?».

Фундаментальным отличием предложенного подхода является отказ от восприятия цифрового доказательства как статического, неизменного артефакта (файла, записи в журнале аудита). В рамках разрабатываемой теории цифровой след рассматривается как результат динамического процесса – функции отображения F объективной реальности R (действия злоумышленника в физическом мире) в цифровую среду D (наблюдаемые данные):

$$D = F(R) + \epsilon, \quad (1)$$

где ϵ – вектор неустранимой погрешности, включающий в себя стохастические возмущения среды (сетевые задержки, асинхронность таймеров), потери данных при логировании и целенаправленные искажения, вносимые средствами анти-форензики.

Следовательно, основной задачей вычислительной форензики становится решение обратной задачи: реконструкция исходного события R по наблюдаемому набору данных D с оценкой доверительного интервала для ϵ. Только при условии, что рассчитанное значение ошибки ϵ находится в допустимых пределах, экспертный вывод может считаться математически верифицированным и юридически значимым.

В этом контексте необходимо особо отметить, что качественная КТЭ должна служить именно установлению онтологической связи между действием (деянием) и последствием. Задача эксперта – предоставить суду возможность дифференцировать временную корреляцию и истинную причинность, доказав, что негативные последствия наступили не просто *после*, а именно *вследствие* конкретного цифрового воздействия. Именно наличие такого математически верифицированного подтверждения причинно-следственной связи выступает необходимым условием для того, чтобы суд, опираясь на выводы эксперта, мог вынести правосудное решение, исключая риск судебной ошибки, основанной на ложной корреляции.

3.2. Базовые принципы доказуемой достоверности. Формирование методологии вычислительной форензики требует введения жёсткой системы критериев, позволяющих провести разделение между научно обоснованным фактом и субъективным экспертным суждением. В условиях состязательного судопроизводства, где цифровые доказательства подвергаются критическому анализу, опора исключительно на профессиональную интуицию эксперта становится источником недопустимых рисков.

Для реализации концепции формальной верификации мы постулируем необходимость базироваться на трёх фундаментальных принципах. Выбор именно этой триады обусловлен требованием изоморфизма между процессом судебного доказывания и процедурой математического вывода: результат должен быть независим от личности исследователя (объективность), содержать оценку погрешности (точность) и допускать независимую проверку логики получения результата (проверяемость).

Таким образом, предлагаемые принципы отличают научный подход от эвристического:

1. Принцип алгоритмической воспроизводимости. Экспертный вывод C должен быть результатом применения детерминированного алгоритма A к исходным данным D_{raw} и базе знаний K: $C = A(D_{raw}, K)$. Это означает, что любой независимый исследователь, обладающий тем же набором D_{raw} и K, обязан получить результат $C' \equiv C$. Любой элемент субъективной оценки («экспертное усмотрение»), не формализованный в виде правила внутри K, признаётся источником неустранимой ошибки.

2. Принцип измеримости неопределённости. Ни одно цифровое доказательство не является абсолютным. Каждое утверждение должно сопровождаться количественной мерой достоверности, рассчитываемой на основе вероятности ложноположительных (*FP*) и ложноотрицательных (*FN*) срабатываний методов обнаружения. Отсутствие метрики достоверности делает вывод юридически ничтожным[3] в контексте байесовского подхода к доказыванию.

3. Принцип формальной верифицируемости. Процесс реконструкции инцидента должен быть изоморфен направленному ациклическому графу, где каждый узел представляет собой доказанный факт, а ребро – причинно-следственную связь. Экспертный вывод

[3] Применительно к заключению эксперта по компьютерным преступлениям «юридически ничтожным» признаётся вывод, в котором специалист, исследуя цифровые артефакты, вместо констатации технических фактов (наличие вредоносного кода, следов сетевого соединения, модификации данных и т.п.) формулирует правовое суждение – например, квалифицирует действия как «неправомерные» или определяет программу как «орудие преступления». Подобные утверждения находятся за пределами предмета судебной компьютерно-технической экспертизы, прямо запрещены законом и УПК РФ, и влекут признание заключения недопустимым доказательством. Подробнее о границах компетенции эксперта см.: Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения. – М.: Право и закон, 2015. – Гл. 2.

считается верифицированным тогда и только тогда, когда существует непрерывный путь от исходных событий (*IoA*) к последствиям (*IoC*), и «прочность» (вес) каждого звена в этой цепи превышает установленный пороговый уровень T_{verif}.

Соблюдение данных принципов является необходимым условием для перехода от вероятностных оценок к детерминированным выводам, что позволяет сформулировать ключевое понятие разрабатываемой теории.

Совокупное выполнение перечисленных принципов формирует базис для введения центральной категории разрабатываемой теории. Если принципы воспроизводимости, измеримости и верифицируемости задают *правила* построения доказательства, то их успешная реализация приводит к достижению особого состояния информационной модели инцидента, которое мы определяем как «цифровая истина». Иными словами, цифровая истина не постулируется априори, а *вычисляется* как результат строгого соблюдения данных принципов при проецировании технических данных на юридическую плоскость.

3.3. Концепция «Цифровой истины». Прежде чем ввести понятие «цифровой истины», необходимо обосновать выбор модели описания инцидента и строго определить соотношение между категориями «инцидент информационной безопасности» и «компьютерное преступление» в рамках предлагаемой методологии.

Инцидент информационной безопасности – это элементарное событие, зафиксированное в цифровой среде и проявляющееся через триаду индикаторов (*IoA, IoB, IoC*, см. ниже), которое *может* служить техническим отражением компьютерного преступления. Это сугубо техническая категория: инцидент ИБ констатирует наличие определённой последовательности цифровых следов, но сам по себе не предопределяет правовую квалификацию.

Компьютерное преступление – это юридическая квалификация общественно опасного деяния, совершённого с использованием информационно-телекоммуникационных технологий. В отличие от единичного инцидента ИБ, компьютерное преступление может охватывать несколько инцидентов, а также включать внешний по отношению к цифровой среде контекст (умысел, мотив, наступившие последствия, не зафиксированные непосредственно в логах). Иными словами, в рамках настоящей работы компьютерное преступление является более широкой категорией: любое компьютерное преступление оставляет в цифровой среде следы, образующие как минимум один инцидент ИБ, однако полная картина преступления может требовать синтеза нескольких инцидентов и внешних данных.

Предлагаемая методология формальной верификации предназначена для проверки гипотез о наличии компьютерного преступления: она реконструирует его структуру и причинные связи путём анализа и агрегирования одного или нескольких инцидентов ИБ в рамках единой онтологической модели. Решающим фильтром, переводящим совокупность технических событий в статус доказанного компьютерного преступления, выступает процедура формальной верификации (см. далее раздел 4).

Мы исходим из того, что любой инцидент информационной безопасности является не сингулярным стохастическим событием, а целенаправленным причинно-следственным процессом. Согласно принципам общей теории систем, такой процесс неизбежно проходит три фазы существования:

1. Фаза потенциала: наличие условий и намерения для совершения действия (причина).
2. Фаза реализации: непосредственное исполнение действия через определённый механизм (процесс).
3. Фаза результата: изменение состояния системы, зафиксированное в материальных носителях (следствие).

Данная онтологическая структура строго изоморфна триаде верификации $IoA \rightarrow IoB \rightarrow IoC$. Таким образом, использование данной модели является не произвольным допущением, а необходимым следствием применения принципа причинности к цифровой среде.

На этом базисе вводится понятие «цифровой истины» как инварианта, сохраняющегося при проекции технических данных на юридическую плоскость. Если принципы (см. п. 3.2) задают процедуру получения знания, то «цифровая истина» характеризует качественное состояние результирующей модели инцидента.

«Цифровая истина» определяется через согласованность элементов триады инцидента:

♦ *IoA* (Indicators of Attack / Affordance) – *Потенциал*: наличие уязвимостей и следов подготовки, создающих возможность для атаки.

♦ *IoB* (Indicators of Behavior) – *Кинетика*: следы действий, описывающие способ реализации умысла (TTPs).

♦ *IoC* (Indicators of Compromise) – *Результат*: артефакты, подтверждающие факт нарушения свойств безопасности (конфиденциальности, целостности, доступности).

Математически «Цифровая истина» достигается при выполнении условия замкнутости контура:

$$Consistency(IoA, IoB, IoC) \to 1. \quad (2)$$

Формально оператор согласованности $Consistency(\cdot)$ представляет собой не бинарную логическую функцию, а меру топологической связности графа инцидента. Условие стремления к единице $\to 1$ означает минимизацию энтропии в цепочке переходов между элементами триады. Обоснуем это утверждение.

Пусть $P(IoB|IoA)$ – условная вероятность реализации конкретного сценария поведения при наличии выявленного потенциала (например, наличие уязвимости и эксплойта), а $P(IoC|IoB)$ – вероятность возникновения наблюдаемых последствий при реализации данного поведения. Тогда интегральный показатель согласованности определяется как произведение вероятностей переходов, взвешенное на коэффициент временной когерентности τ:

$$Consistency \approx P(IoB|IoA) \times P(IoC|IoB) \times \tau(t_{IoA}, t_{IoB}, t_{IoC}), \quad (3)$$

где τ – функция, принимающая значение 1 при строгом соблюдении хронологии ($t_{IoA} < t_{IoB} < t_{IoC}$) и 0 при её нарушении.

Таким образом, условие $Consistency \to 1$ требует одновременного выполнения трёх жёстких ограничений:

1. Детерминированность: Наблюдаемое действие (IoB) должно быть прямым следствием возможности (IoA), а не случайным событием.
2. Результативность: Последствие (IoC) должно быть закономерным итогом действия (IoB), исключая появление артефактов "из ниоткуда".
3. Хронологическая истинность: Причинно-следственная стрела времени не должна быть нарушена.

Только в том случае, когда произведение этих вероятностей стремится к максимуму, мы можем утверждать, что реконструированная модель инцидента изоморфна реальному событию, а значит обладает свойством «цифровой истины». Любое отклонение от единицы ($Consistency < 1 - \delta$) свидетельствует о наличии разрыва между данными и правовой нормой, что делает экспертный вывод юридически ничтожным.

Ситуация, при которой обнаружен *IoC* (факт взлома), но отсутствует соответствующий *IoB* (трасса действий) или *IoA* (вектор атаки), классифицируется как «семантический разрыв», указывающий на неполноту собранных для анализа данных, низкую достоверность версии или наличие признаков фальсификации (анти-форензики).

3.4. Теоретико-множественный подход к преодолению семантического разрыва. Центральной проблемой обеспечения юридической значимости экспертного вывода является преодоление «семантического разрыва» – отсутствия взаимно-однозначного соответствия между дискретными техническими событиями и абстрактными правовыми категориями.

В основу онтологической модели положены результаты авторов, впервые сформулированные в [28, 29] и кратко воспроизводимые здесь для связности изложения. Опираясь на результаты исследований по онтологическому моделированию инцидентов [28], мы предлагаем решать данную проблему через введение формализма структурной проекции.

Постулируется, что любой юридически значимый компьютерный инцидент (то есть такой, который при успешной верификации может быть квалифицирован как компьютерное преступление) может быть описан упорядоченным кортежем, изоморфным составу преступления:

$$CI = \langle S, M, O, R_{cause} \rangle, \quad (4)$$

где элементы множества формируются путём агрегации низкоуровневых индикаторов:

1. S (Subject/Субъект) – проекция множества индикаторов атаки (*IoA*). Описывает цифровую личность и умысел:

$$S = \{x \in IoA \mid is\_attribution(x)\}.$$

2. M (Method/Способ) – проекция множества индикаторов поведения (*IoB*). Описывает технический алгоритм реализации угрозы (TTPs).

$$M = \{y \in IoB \mid is\_technique(y)\}.$$

3. O (Object/Объект) – проекция множества индикаторов компрометации (IoC). Описывает нарушение свойств безопасности актива.

$$O = \{z \in IoC \mid affected(z)\}$$

4. R_{cause} – отношение причинности, утверждающее, что конкретная техника $m_j \in M$ привела к конкретному последствию $o_k \in O$.

В терминах уголовного права эта формальная структура получает исчерпывающую семантическую интерпретацию, образуя мост между техническими данными и составом преступления.

Субъект (S) проецируется на признаки субъекта преступления и субъективную сторону деяния. Технические идентификаторы (IP-адреса, учётные записи), извлекаемые из индикаторов атаки, формируют цифровой профиль, позволяющий идентифицировать лицо, совершившее деяние; контекстные признаки (аномальное время, сессионные артефакты) указывают на наличие умысла – приготовления и разведки. Тем самым S служит техническим отображением виновного деяния.

Способ (M) проецируется на объективную сторону преступления – способ его совершения. Выявляемые через индикаторы поведения цепочки тактик и техник (TTPs) восстанавливают алгоритм действий злоумышленника от проникновения до реализации угрозы, т.е. фиксируют «механизм преступления». Это позволяет соотнести техническую активность с диспозицией конкретной статьи УК РФ.

Объект (O) проецируется на объект преступления и его последствия. Зафиксированные через индикаторы компрометации факты нарушения конфиденциальности, целостности или доступности информации образуют материальный признак состава, а пострадавшие активы – предмет посягательства. Множество O даёт формальное основание для вывода о наступлении общественно опасных последствий.

Причинная связь (R_{cause}) формализует обязательный элемент объективной стороны материальных составов (ст. 272, 274 УК РФ). Отношение $M \to O$ доказывает, что наблюдаемый ущерб наступил именно в результате реализации установленного способа, а не вследствие случайного совпадения или действий третьих лиц. Тем самым устраняется подмена причинности временной корреляцией.

Именно эта проекция позволяет преодолеть разрыв между данными и правовой нормой: технические индикаторы перестают быть изолированными событиями и приобретают значение юридически значимых элементов, непосредственно соотносимых с предметом доказывания по уголовному делу.

Решение проблемы неполноты данных. Традиционная экспертиза, базирующаяся на сигнатурном поиске («объектный подход»), оказывается бессильной в ситуациях, когда один из элементов (обычно IoC – вредоносный файл) уничтожен средствами антифорензики. В терминологии нашей теории это означает разрыв в множестве наблюдаемых фактов (O=∅) [29].

Разрабатываемая теория формальной верификации предлагает решение через анализ связности графа причинности (R_{cause}). Поскольку модель инцидента представляет собой направленный ациклический граф $S \to M \to O$, истинность события может быть доказана через транзитивность связей, даже при отсутствии отдельных узлов [28].

Вводится *Аксиома сохранения следа процесса:*

«Невозможно реализовать изменение состояния системы O (ущерб) без реализации процесса M (способа), порождающего динамические следы в оперативной памяти и журналах аудита, инвариантные к удалению статических файлов».

Математически это означает, что верификация инцидента возможна, если выполняется условие существования отображения:

$$\exists m \in M: (m \to Impact) \in R_{cause}. \quad (5)$$

В качестве примера рассмотрим расследование «бесфайловых» атак типа LotL, где отсутствуют вредоносные файлы (IoC – пусто или неинформативно), алгоритм реконструирует инцидент по вектору $S \to M$ (цепочка запуска легитимных утилит PowerShell с аномальными аргументами). Если расчётный коэффициент K_{link} для цепочки M превышает порог достоверности, система верифицирует инцидент как «Неправомерный доступ» (ст. 272 УК РФ), математически доказывая способ совершения преступления без предъявления «орудия» (файла) [28].

Таким образом, интерпретационный разрыв преодолевается путём перехода от поиска *изолированных артефактов* к доказательству *целостности структуры* (*S-M-O*). Это позволяет трансформировать неопределённость в верифицируемую вероятностную оценку.

4. Методология формальной верификации экспертных выводов. В отличие от задач обнаружения, решаемых средствами защиты информации, или задач расследования, решаемых оператором, задача формальной верификации имеет иную математическую природу.

Мы постулируем, что реконструкция инцидента по цифровым следам относится к классу обратных некорректных задач в определении А.Н. Тихонова [30]. Как показано в работах по теории цифровых расследований [31], некорректность обусловлена необратимой потерей информации (энтропией) при проекции событий физического мира в цифровую среду, что делает решение неустойчивым: малые возмущения в исходных данных (шум, анти-форензика) могут приводить к произвольно большим ошибкам в выводах.

Следовательно, цель верификации – это регуляризация решения обратной задачи, обеспечивающая валидацию истинности утверждений. В рамках парадигмы вычислительной форензики [6] и теории формальных доказательств [32], экспертный вывод *C* рассматривается не как нарратив, а как логическая пропозиция, истинность которой должна быть доказана (верифицирована) относительно модели причинности [33] и имеющихся данных *D*.

4.1. Постановка задачи верификации. Пусть экспертный вывод *C* представляет собой утверждение о существовании инцидента с определёнными характеристиками. Формально *C* моделируется как кортеж гипотез, базирующийся на онтологической модели *S-M-O*, предложенной в работе [28]:

$$C = \langle H_S, H_M, H_O, H_{link} \rangle, \tag{6}$$

где H_S, H_M, H_O – гипотезы о Субъекте, Способе и Объекте соответственно, а H_{link} – гипотеза о наличии причинно-следственной связи между ними.

Целевой функцией методологии является бинарный предикат валидности $Verif(C)$ [32], принимающий значение «Истина» тогда и только тогда, когда выполняется система из четырёх критериев качества:

$$Verif(C) = I_{struct}(C) \wedge I_{cause}(C) \wedge I_{consist} \wedge I_{ground}(C), \tag{7}$$

где I_{struct} – критерий структурной полноты (соответствие составу); I_{cause} – критерий причинно-следственной связности (сила связи); $I_{consist}$ – критерий непротиворечивости (отсутствие конфликтов); I_{ground} – критерий фактической обоснованности (трассируемость).

4.2. Критерий 1: Проверка структурной полноты (I_{struct}). Данный этап проверяет семантическую корректность вывода. Экспертное заключение не может считаться верифицированным, если в нём отсутствуют элементы, обязательные для квалификации деяния согласно УК РФ.

Методология предполагает проекцию гипотезы *C* на онтологический шаблон преступления T_{crime}. Здесь под T_{crime} понимается множество обязательных элементов состава преступления, изоморфное структуре кортежа *CI* и включающее Субъекта, Способ, Объект и отношение причинности (R_{cause}), как это определено в разделе 3.4. Использование онтологического маппинга для стандартизации понятий обосновано в работах **[**19**]** и **[**20**]**. Вывод признаётся структурно полным, если установлено сюръективное отображение множества выявленных фактов на множество элементов состава преступления (онтологический шаблон T_{crime}):

$$I_{struct}(C) = \begin{cases} 1, & \text{если } \forall e \in T_{crime} \exists h \in C : match(h, e) \\ 0, & \text{иначе} \end{cases}. \tag{8}$$

Практический смысл: система автоматически блокирует выводы вида «произошёл взлом» (есть H_O), если не установлен способ взлома (H_M отсутствует), классифицируя такой вывод как юридически несостоятельный.

Следует отметить, что критерий I_{struct} в текущей версии методологии является бинарным: он требует обязательного наличия всех элементов состава преступления в экспертном выводе. Это жёсткое условие гарантирует юридическую строгость для задач уголовного судопроизводства, но может оказаться чрезмерно консервативным в иных контекстах (например, на ранних этапах расследования или в оперативном мониторинге). Практика показывает, что неполнота идентификации субъекта при установленных способе и последствиях не всегда должна приводить к полному отказу от использования вывода – скорее, она должна понижать степень категоричности до вероятностной.

В рамках предложенной математической модели данное требование может быть смягчено без нарушения общей архитектуры. Коэффициент γ, введённый в функцию доверия (раздел 5.1) как штраф за энтропию среды, уже демонстрирует механизм количественного учёта неопределённости. В перспективе его действие может быть расширено: структурная неполнота (например, отсутствие атрибутов субъекта) может интерпретироваться как дополнительный источник энтропии, увеличивая эффективное значение E_{sys} либо непосредственно корректируя вклад I_{struct} через весовые коэффициенты в итоговом предикате $Verif(C)$. Это позволило бы не отвергать гипотезу целиком, а понижать её доверительную оценку, сохраняя непрерывность шкалы при переходе от полных структур к неполным. Формальная реализация такого расширения составляет предмет отдельного исследования.

4.3. Критерий 2: Проверка каузальной связности (I_{cause}). Это ядро методологии. Эксперт часто подменяет причинность корреляцией («после» не значит «вследствие»). Методология верификации требует математического доказательства того, что реализация способа H_M является *необходимым и достаточным условием* наступления последствия H_O.

Для реализации этого требования мы адаптируем аппарат графов атак, развитый в работах [25] и [24], дополняя его элементами теории вероятностной причинности [33]. Вводится метрика *коэффициент причинности* (K_{Link}), рассчитываемая на графе переходов состояний системы:

$$K_{Link}(H_M \to H_O) = P(O|M, Context) \cdot \big(1 - H(noise)\big), \tag{9}$$

где $P(O|M)$ – условная вероятность перехода (из базы знаний MITRE ATT&CK), а $H(noise)$ – энтропия (зашумлённость) среды, рассчитываемая по методике **[**22**]**.

Условие верификации:

$$I_{cause}(C) = (K_{Link} \geq K_{threshold}). \tag{10}$$

Если расчётный коэффициент K_{Link} ниже порога $K_{threshold}$ (например, 0.95 для категорического вывода), связь признаётся недоказанной, а вывод – вероятностным, но не категорическим.

4.4. Критерий 3: Проверка непротиворечивости ($I_{consist}$). Данный критерий проверяет внутреннюю логическую и хронологическую целостность модели. Даже если факты подтверждены логами (I_{ground}), их совокупность может содержать парадоксы, указывающие на фальсификацию или ошибку интерпретации. Проверка формализуется как задача удовлетворения ограничений. Вводятся два типа инвариантов:

1. Хронологические инварианты (τ): Событие-причина всегда предшествует событию-следствию.

$$\forall\big(h_i, h_j\big) \in C\colon \big(h_i \to h_j\big) \Longrightarrow \Big(t_{start}(h_i) \leq t_{start}\big(h_j\big)\Big). \tag{11}$$

Пример конфликта: Время создания файла (t_{create}) позже времени его последнего изменения (t_{mod}), что невозможно в штатном режиме работы файловой системы NTFS/EXT4.

2. Семантические инварианты (Σ): Атрибуты взаимодействующих сущностей должны быть совместимы.

$$Compatibility\left(Attr(h_i), Attr\big(h_j\big)\right) = True. \tag{12}$$

Пример конфликта: Гипотеза утверждает, что Субъект использовал эксплойт для уязвимости Windows (SMBv1), но Объект функционирует под управлением Linux.

Условие верификации:

$$I_{consist}(C) = \bigwedge\nolimits_{\forall h \in C}(\neg Conflic\, t_{\tau}(h) \wedge \neg Conflict_{\Sigma}(h)). \tag{13}$$

Здесь $Conflict_{\tau}(h)$ – предикат, принимающий значение «истина», если существует такая гипотеза $h' \in C$, что пара (h, h') нарушает хотя бы один хронологический инвариант τ. Аналогично, $Conflict_{\Sigma}(h)$ фиксирует наличие семантического конфликта гипотезы h с любой другой гипотезой из C. Таким образом, требование $\neg Conflict_{\tau}(h) \wedge \neg Conflict_{\Sigma}(h)$ означает, что гипотеза h не вступает в противоречие ни с одной из остальных гипотез ни по времени, ни по атрибутам взаимодействующих сущностей. Конъюнкция по всем $h \in C$ обеспечивает глобальную непротиворечивость вывода.

4.5. Критерий 4: Проверка фактической обоснованности (I_{ground}). Данный критерий проверяет, что каждый элемент гипотезы C опирается на объективные данные первичных измерений D_{raw}. Это реализация принципа «прослеживаемости доказательств» (трассировки), сформулированного в работе [21].

Для каждого элемента $h \in C$ строится цепочка трассируемости к исходному дампу памяти или журналу аудита. Верификация проходит успешно, если мощность множества неподтверждённых гипотез равна нулю:

$$I_{ground}(C) \Leftrightarrow \{h \in C \mid \nexists d \in D_{raw}: support(d, h)\} = \emptyset.$$

4.6. Процедура принятия решения. Итоговая методология формальной верификации реализуется как последовательный алгоритм:

1. Синтаксический контроль: Проверка I_{struct}. Если выявлен дефицит структуры (например, нет мотива), вывод возвращается на доработку.
2. Семантический контроль: Расчёт K_{Link} для всех рёбер графа. Если связь слабая, система понижает статус вывода с «Категорический» до «Вероятностный».
3. Фактологический контроль: Проверка ссылочной целостности доказательств (I_{ground}).

Результатом применения методологии является *сертификат верификации* – метаданные, содержащие математическое обоснование надёжности экспертного вывода. Это позволяет суду оценить допустимость доказательства не на основе веры в авторитет эксперта, а на основе объективных метрик, что соответствует подходу «доказуемой безопасности» [25].

5. Математическая модель оценки достоверности. Описанная выше методология верификации требует формализации в виде математической модели, позволяющей перейти от бинарной логики («верифицировано/не верифицировано») к непрерывной шкале оценки доверия. Это обусловлено тем, что в задачах вычислительной форензики, как отмечает К. Франке, мы всегда оперируем в пространстве вероятностей, а не абсолютных истин [6].

5.1. Функция доверия к гипотезе. Введём понятие функции доверия $Trust(H)$, которая отображает экспертную гипотезу H на единичный отрезок $[0, 1]$. Данная функция является агрегатором трёх независимых метрических показателей, характеризующих различные аспекты инцидента.

Предлагается следующая концептуальная формула оценки достоверности:

$$Trust(H) = f\left(W_{match}, K_{Link}, E_{sys}\right), \quad (14)$$

где W_{match} – метрика таксономического соответствия. Характеризует степень совпадения (изоморфизма) выявленных следов с эталонными профилями атак (например, паттернами MITRE ATT&CK), описанными в онтологии. Этот показатель опирается на методы векторной идентификации, разрабатываемые в смежных исследованиях [28]. Смысл метрики – насколько то, что мы наблюдаем, похоже на известную атаку?

K_{Link} – коэффициент силы причинной связи. Динамический параметр, рассчитываемый на графе инцидента (см. Раздел 4.3). Он отражает вероятность того, что последовательность событий не является случайной. Смысл коэффициента – насколько прочно события связаны между собой логикой и временем?

E_{sys} – Энтропия наблюдаемой среды. Показатель зашумлённости и неопределённости данных, рассчитываемый на основе подходов, предложенных в работах по метрикам безопасности [22]. Высокая энтропия (хаотичность логов, отсутствие временных меток) снижает доверие к выводу, даже если паттерн (W_{match}) выглядит убедительно.

Итоговая решающая функция может быть представлена в виде аддитивно-мультипликативной модели с весовыми коэффициентами регуляризации α, β, γ:

$$Trust(H) = \frac{1}{1+e^{-(\alpha \cdot W_{match} + \beta \cdot K_{Link} - \gamma \cdot E_{sys})}}. \quad (15)$$

В данной модели сигмоида выполняет роль функции активации экспертного вывода: она переводит гипотезу из «спящего» состояния (накопление улик) в «активное» (доказанный факт), когда взвешенная сумма доказательств превышает порог сопротивления энтропии.

5.1.1. Семантическая интерпретация и методика калибровки весовых коэффициентов. Введённые в уравнение доверия коэффициенты регуляризации α, β, γ являются не произвольными константами, а *гиперпараметрами модели*, определяющими чувствитель-

ность системы верификации к различным классам доказательств. Их физический смысл и способ определения базируются на принципах логистической регрессии и экспертного оценивания [10].

1. Семантика коэффициентов:

α – Коэффициент доверия к методу обнаружения. Характеризует надёжность источника, зафиксировавшего совпадение с таксономией (W_{match}). Если W_{match}получен от сертифицированного средства защиты (например, SIEM с актуальными базами), $\alpha \to max$. Если паттерн выявлен эвристическим анализатором с высоким уровнем ошибок I рода, значение α снижается. Усиливает вклад «факта» наличия улики.

β – Коэффициент значимости причинности. Определяет «вес» логической связности в итоговом решении. В задачах квалификации материальных составов преступлений (ст. 272, 274 УК РФ), где доказывание причинно-следственной связи является обязательным, β принимает доминирующее значение ($\beta > \alpha$). Это математически выражает тезис: «Связь важнее, чем отдельный факт». Блокирует принятие решения при разрывах в графе, даже если найдено множество разрозненных артефактов.

γ – Коэффициент штрафа за неопределённость. Параметр регуляризации, отвечающий за консерватизм системы. Чем агрессивнее среда (наличие признаков антифорензики, отсутствие журналов аудита), тем выше должно быть значение γ. Это позволяет искусственно занижать доверие $Trust(H)$ в «грязных» средах, требуя более веских доказательств для компенсации энтропии. Реализует принцип презумпции невиновности (сомнения толкуются в пользу обвиняемого) – в условиях высокой энтропии система скорее откажет в верификации, чем даст ложноположительный вывод. Отрицательный знак перед γ в формуле (15) это принципиальное выражение того, что энтропия среды *вычитается* из совокупной силы доказательств, обеспечивая консервативность модели в соответствии с презумпцией невиновности

2. Методика выбора значений:

Для определения численных значений коэффициентов предлагается гибридный подход, сочетающий метод экспертных оценок и обучение на прецедентах.

Этап А. Экспертная инициализация (метод анализа иерархий) [34].

На этапе холодного старта коэффициенты рассчитываются на основе матриц парных сравнений, заполняемых квалифицированными экспертами-криминалистами.

Пример соотношения для типовых задач:

- Для автоматизированного поиска: $\alpha = 1.0, \beta = 0.5, \gamma = 0.2$ (важно ничего не пропустить, ложные срабатывания допустимы).
- Для судебной экспертизы: $\alpha = 0.8, \beta = 1.5, \gamma = 1.2$ (критически важна причинность и отсутствие сомнений).

Этап Б. Алгоритмическая оптимизация.

При наличии размеченного датасета (архива расследованных инцидентов с известным вердиктом $y \in \{0,1\}$) задача сводится к обучению классификатора. При накоплении достаточного объёма размеченных данных возможна алгоритмическая донастройка весов методом градиентного спуска. Коэффициенты $w = \{\alpha, \beta, -\gamma\}$ находятся путём минимизации функции потерь [12]:

$$L(w) = -\sum_i [y_i \ln(\mathrm{Trust}(H_i)) + (1 - y_i)\ln(1 - \mathrm{Trust}(H_i))] \to min. \quad (16)$$

Полученные таким образом значения являются математически оптимальными для конкретного типа инфраструктуры и профиля угроз.

5.1.2 Выбор функции активации. Применение в (15) сигмоидальной функции активации позволяет интерпретировать результат как вероятность истинности гипотезы $P(H \mid E)$. Выбор логистической функции $\sigma(z) = \frac{1}{1+e^{-z}}$ обусловлен необходимостью математического моделирования перехода от количественной меры доказательств к качественной форме экспертного вывода, что соответствует вероятностной интерпретации логистической регрессии [10]. Данное преобразование позволяет агрегировать разнородные метрики (время, энтропию, таксономию) в единую вероятностную оценку, необходимую для принятия юридически значимого решения.

В теории судебной экспертизы принято выделять категорические (однозначные) и вероятностные (предположительные) выводы [5]. Однако цифровые следы, являясь результатом стохастических процессов в вычислительной среде, изначально имеют вероятностную природу.

Сигмоидальная функция позволяет корректно отобразить непрерывное пространство состояний доказательной базы $(-\infty, +\infty)$ на нормированный интервал оценки достоверности [0, 1], обеспечивая дифференциацию формы вывода:

1. Зона категорической определённости: При значениях аргумента $z \to +\infty$, функция асимптотически приближается к 1. Это соответствует ситуации, когда совокупность доказательств (W_{match}, K_{Link}) настолько превышает уровень энтропии (E_{sys}), что вероятность ошибки становится пренебрежимо малой $(P_{err} < \varepsilon)$. В этой зоне формируется категорический положительный вывод.
2. Зона вероятностного суждения: На участке линейного роста функции (центральная часть графика сигмоиды) малые изменения в доказательной базе существенно влияют на итоговое значение. Значения *Trust(H)* в диапазоне (например, $0.7 \ldots 0.95$) интерпретируются как вероятностный вывод высокой степени обоснованности.
3. Зона НПВ (Не представилось возможным): Значения около 0.5 свидетельствуют о паритете доказательств и шума, что требует отказа от дачи заключения или формулирования вывода в форме НПВ.

Таким образом, сигмоида выступает «решающим правилом», которое трансформирует взвешенную сумму технических аргументов в процессуально значимую форму вывода.

5.2. Дифференциация инцидентов и легитимной активности. Ключевой проблемой автоматизированных средств является высокий уровень ложноположительных срабатываний, когда легитимные действия администратора квалифицируются как инцидент. Рассмотрим, как введённая модель решает эту задачу (табл. 1).

Пример: Использование утилиты PowerShell для удалённого управления (техника T1059).

Сценарий А (Администратор): Системный администратор запускает скрипт обслуживания в рабочее время.

Сценарий Б (Злоумышленник): Атакующий запускает обфусцированный скрипт для эксфильтрации данных.

Таблица 1

Сравнительный анализ верификации сценариев

Параметр модели	**Сценарий А (Легитимный администратор)**	**Сценарий Б (Атака LoTL)**	**Комментарий модели**
W_{match}	Высокий (0.9). Паттерн совпадает с техникой T1059.	Высокий (0.9). Паттерн совпадает с техникой T1059.	Сигнатурный/эвристический анализ не видит разницы (оба используют PowerShell).
K_{Link}	Низкий (0.2). Цепочка обрывается. Действие *M* не ведёт к ущербу *O* (нет нарушения КЦД). Есть связь с легитимным тикетом в Service Desk (контекст).	Высокий (0.95). Действие *M* имеет причинную связь с аномальным исходящим трафиком (*O*). Соблюдена хронология $t_{IoB} < t_{IoC}$.	Верификация через причинность выявляет разрыв в легитимном сценарии (нет состава преступления).
E_{sys}	Низкая (0.1). Стандартная среда, логи целостны.	Средняя/Высокая (0.6). Наличие признаков антифорензики (очистка журналов), таймстомпинг.	Энтропия понижает доверие к версии о «случайном сбое» в Сценарии Б.
Итог $Trust(H)$	$Trust(H) < T_{verif}$ (Отказ)	$Trust(H) \to T_{verif}$ (Верифицировано)	
Вывод	Событие классифицируется как «Технологическая операция».	Событие квалифицируется как «Неправомерный доступ» (ст. 272 УК РФ).	

Рассмотрим две гипотезы, соответствующие сценариям из табл. 1:

- H_A: легитимное обслуживание (администратор),
- H_B: неправомерный доступ (LotL-атака).

Пусть для H_A по исходным данным получены следующие метрики:

$$W_{match} = 0.9, K_{Link} = 0.2, E_{sys} = 0.1.$$

Для H_B соответственно:

$$W_{match} = 0.9, K_{Link} = 0.95, E_{sys} = 0.6.$$

При стандартных весах для судебной экспертизы (раздел 5.1.1): $\alpha = 0.8$, $\beta = 1.5$, $\gamma = 1.2$ и пороге $T_{verif} = 0.95$ вычислим $Trust(H)$ по формуле (15):

$$z_A = 0.8 \cdot 0.9 + 1.5 \cdot 0.2 - 1.2 \cdot 0.1 = 0.72 + 0.3 - 0.12 = 0.90$$

$$Trust(H_A) = \frac{1}{1 + e^{-0.90}} \approx 0.71$$

$$z_B = 0.8 \cdot 0.9 + 1.5 \cdot 0.95 - 1.2 \cdot 0.6 = 0.72 + 1.425 - 0.72 = 1.425$$

$$Trust(H_B) = \frac{1}{1 + e^{-1.425}} \approx 0.806$$

Однако для уголовного судопроизводства $T_{verif} = 0.95$, и обе гипотезы не достигают порога. Это ожидаемо: в первом случае не выполнена причинная связь, во втором – высокая энтропия среды требует дополнительных доказательств. При снижении энтропии, например, до $E_{sys} \approx 0.1$ (после восстановления логов), $Trust(H_B)$ возрастает, всё ещё оставаясь вероятностным. Категорический вывод потребовал бы $K_{Link} \to 1$ при $E_{sys} \to 0$.

Таким образом, введение параметров K_{Link} и E_{sys} позволяет математически отсечь ложноположительные срабатывания, возникающие при использовании только сигнатурных методов (W_{match}), и обеспечить семантическую корректность экспертного вывода.

На рис. 1 представлена итоговая диаграмма потока данных от фиксации следов инцидента к принятию решения о верификации выводов КТЭ, иллюстрирующая подразделы 5.1-5.2:

1. Входные потоки: слева и справа подаются данные (следы) и знания (онтология).
2. Параллельные вычисления: явно выделены три независимых процесса, которые описаны в подразделах 5.1-5.2:
   - *Векторная идентификация* даёт значение W_{match} (насколько это похоже на инцидент).
   - *Каузальный анализ* даёт значение K_{Link} (связано ли это причинной связью).
   - *Энтропийный анализ* даёт значение E_{sys} (не подделано ли это).
3. Математическое ядро: Блок с формулой сигмоиды, где происходит взвешивание показателей (коэффициенты α, β, γ).
4. Логический выход: Бинарное решение на основе порога T_{verif}.

Здесь необходимо уточнить, что $K_{threshold}$ (10) является частным порогом для причинной связи, а T_{verif} – интегральным порогом для итоговой достоверности.

5.2.1. Калибровка порога принятия решений T_{verif}. Выбор граничного значения T_{verif}, разделяющего гипотезы на верифицированные и отвергнутые, не является технической константой, а диктуется правовым стандартом доказывания, применимым к конкретной юрисдикции.

С точки зрения байесовской теории принятия решений, порог T_{verif} определяется через минимизацию ожидаемого риска, зависящего от соотношения «цены» ошибок I и II рода:

$$T_{verif} = \frac{Cost(FP)}{Cost(FP) + Cost(FN)}, \quad (17)$$

где $Cost(FP)$ – ущерб от ложного обвинения (False Positive), а $Cost(FN)$ – ущерб от пропуска инцидента (False Negative).

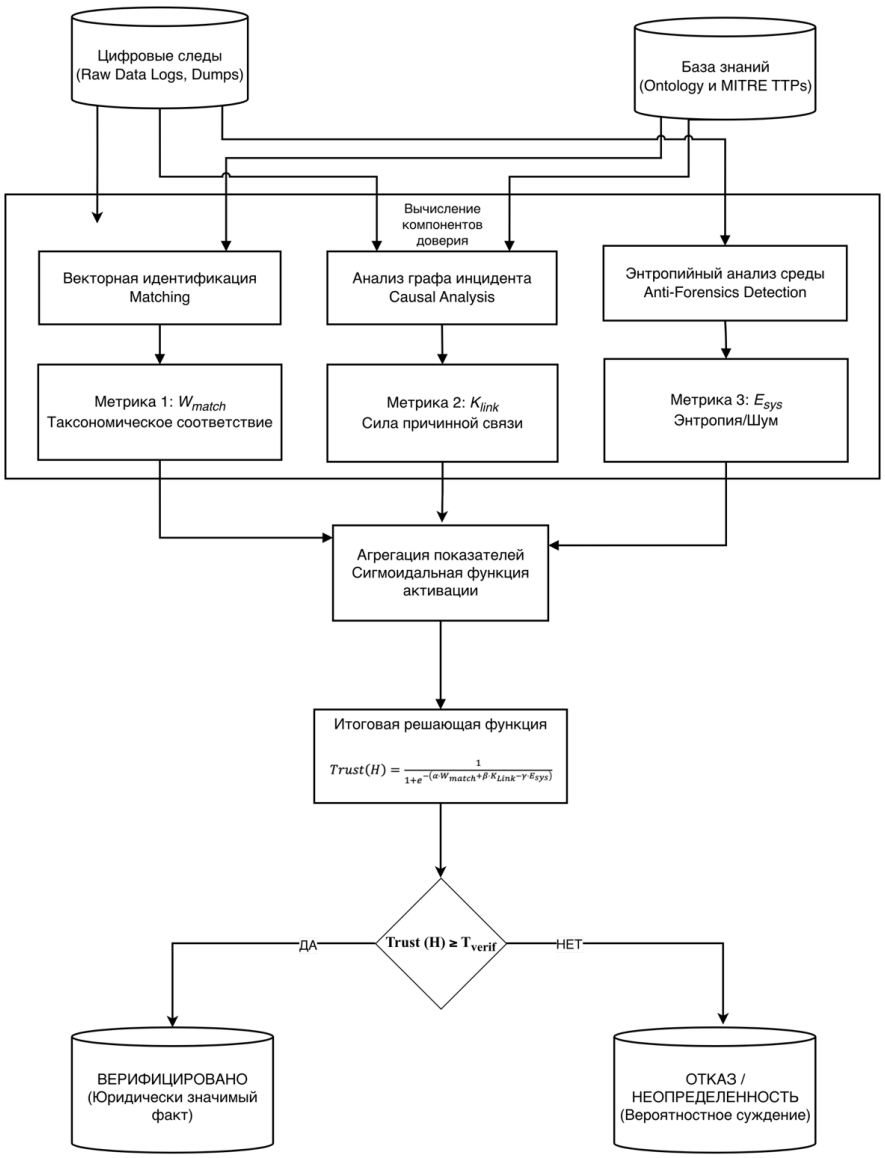

Рис. 1. Диаграмма потока данных от следов к принятию решения

Методика настройки:

В программной реализации системы верификации значение T_{verif} должно задаваться как внешний конфигурационный параметр, выбираемый экспертом исходя из фабулы дела:

- Если система используется для фильтрации событий в SOC, устанавливается мягкий порог (0.7), чтобы минимизировать пропуски атак.
- Если система используется для формирования судебного заключения, активируется жёсткий порог (0.95), обеспечивающий фильтрацию любых сомнительных гипотез в соответствии с презумпцией невиновности.

Таким образом, модель обеспечивает гибкость, позволяя использовать единый математический аппарат ($Trust(H)$) для решения задач разного уровня ответственности.

В табл. 2 приведены рекомендуемые значения порогов для различных классов задач, полученные путём проекции юридических стандартов на вероятностную шкалу модели.

Таблица 2

Адаптация порога верификации под правовой контекст

Тип процесса / Задача	Юридический стандарт[4]	Цена ошибки	Рекомендуемый порог T_{verif}
Уголовное судопроизводство (ст. 272.х-274.х УК РФ)	Beyond Reasonable Doubt («Вне разумных сомнений»). Требует практически полной уверенности, так как цена ложного обвинения максимальна (лишение свободы).	$Cost(FP) \gg Cost(FN)$	≥ 0.95 (Зона категорического вывода)
Арбитраж и гражданский процесс (Убытки, споры хозяйствующих субъектов)	Preponderance of the Evidence («Баланс вероятностей» или «Перевес доказательств»). Достаточно, чтобы версия истца была более вероятна, чем версия ответчика.	$Cost(FP) \approx Cost(FN)$	> 0.51 (Зона вероятностного вывода)
Оперативный мониторинг (SOC) / Incident Response	Reasonable Suspicion («Обоснованное подозрение»). Задача – не пропустить атаку, ложные срабатывания допустимы для перестраховки.	$Cost(FN) > Cost(FP)$	≈0.70 (Зона оперативного реагирования)

6. Обсуждение результатов. Разработанная методология формальной верификации компьютерных инцидентов направлена на разрешение фундаментального противоречия цифровой криминалистики: конфликта между дискретной природой машинных данных и оценочным характером юридических суждений. Проведённый анализ научной литературы (см. раздел 2.2) подтверждает, что предлагаемый подход закрывает существующий методологический пробел и вводит в научный оборот ранее не формализованный аппарат оценки достоверности экспертных выводов.

Ниже приведён анализ преимуществ, ограничений и правового статуса предлагаемого подхода с опорой на современные исследования.

6.1. Трансформация экспертного вывода: от «мнения» к «доказательству». Ключевым достижением предлагаемого подхода является смена парадигмы формирования экспертного заключения. Современная практика расследования всё ещё сильно зависит от субъективного фактора, когда эксперт полагается на личный опыт и интуицию, а суд при анализе качества заключения – на репутацию и регалии эксперта. Как показывают исследования, эксперты часто скептически относятся к автоматизированным средствам, требуя высокого уровня валидации решений для исключения ошибок [35].

Внедрение функции доверия $Trust(H)$ и порогового критерия T_{verif} позволяет перейти к модели «доказуемой экспертизы»:

1. Объективизация и воспроизводимость. Традиционные методы интерпретации разрозненных данных вручную становятся неэффективными в условиях роста объёма следов. Формализация процесса классификации исключает «человеческий фактор» и обеспечивает воспроизводимость результата экспертизы, что является ключевым требованием валидации методик.
2. Снижение вероятности ошибок. Эмпирические исследования подтверждают, что автоматизированные методы предварительного анализа способны снизить количество ошибок при принятии решений об исключении вещественных доказательств. Предлагаемая модель математически закрепляет этот эффект, блокируя выводы, не имеющие достаточной каузальной поддержки.

[4] Термины «Beyond Reasonable Doubt», «Preponderance of the Evidence» и «Reasonable Suspicion» обозначают устоявшиеся в процессуальной доктрине стандарты доказывания – пороговые критерии, определяющие степень убеждённости суда (или иного правоприменителя), достаточную для признания юридического факта установленным. В странах общего права они образуют формализованную иерархию, однако их концептуальное содержание активно исследуется и применяется (в том числе де-факто) в российской науке и правоприменительной практике (см. Сидорова Н.А., Васильев И.А. Применение стандартов доказывания при вынесении процессуальных решений по уголовным делам // Вестник СПбГУ. Право. 2025. № 3).

6.2. Технические ограничения и границы применимости. Несмотря на преимущества, методология обладает рядом ограничений, обусловленных природой современных киберугроз:

1. Проблема полноты онтологической модели. Эффективность верификации зависит от того, насколько полно база знаний описывает ландшафт угроз. Существующие таксономии (например, MITRE ATT&CK) описывают механику атаки, но не структуру преступления. Если атакующий применяет принципиально новую технику (Zero-Day) или легитимные инструменты в рамках атак LoTL, сигнатурные методы и стандартные онтологии могут не выявить аномалий, что приводит к «слепым зонам» в расследовании.

2. Противодействие расследованию (анти-форензика). Злоумышленники активно применяют методы уничтожения статических следов (вайпинг, бесфайловые атаки в оперативной памяти). В таких условиях модель, ориентированная только на поиск файлов (*IoC*), оказывается уязвимой. Решением является перенос фокуса на поведенческие индикаторы (*IoB*), которые сложнее фальсифицировать, так как они отражают логику атаки, а не её инструменты.

Атака на модель верификации. Предлагаемая методология разделяет процесс выдвижения гипотез (прерогатива эксперта) и их формальную оценку (функция модели). В этом контексте необходимо разграничивать два класса противодействия. Анти-форензика, направленная на сокрытие или искажение следов конкретного преступления, влияет на входные данные, но не компрометирует аппарат верификации: модель оценит гипотезу относительно доступных данных, и при неполноте структуры (например, отсутствии M) закономерно откажет в категорическом выводе. Более изощрённый класс угроз – целенаправленная атака на саму модель, при которой злоумышленник, зная структуру онтологии, пороговые значения и весовые коэффициенты, фабрикует следовую картину так, чтобы ложная гипотеза получила высокую оценку $Trust(H)$, а истинная – низкую. Такая атака требует от злоумышленника значительного контроля над цифровой средой и осведомлённости о математическом аппарате, что в реальных условиях труднодостижимо.

Однако данная уязвимость не является неустранимой. Искусственное конструирование «идеальной» следовой картины или, напротив, стерильное уничтожение следов часто порождает статистически обнаружимые аномалии в энтропийном профиле цифровых артефактов. В отечественной науке предложен статистический метод обнаружения локальных неоднородностей данных, основанный на анализе энтропийных характеристик и позволяющий выявлять «идеально случайные» фрагменты, характерные для работы инструментов сокрытия [36]. В англоязычной литературе также развиваются подходы к обнаружению аномалий без априорной статистической модели – с использованием информационных мер на базе алгоритмов сжатия Лемпеля-Зива [37], а также методов приоритизации артефактов на основе логарифмической энтропии [38]. Интеграция подобных процедур в контур верификации позволит модели не только оценивать достоверность гипотезы, но и выявлять признаки направленной атаки на саму процедуру оценки, что составляет предмет дальнейших исследований.

Отдельного упоминания заслуживает вопрос вычислительной сложности. Расчёт энтропии среды E_{sys} и коэффициента K_{Link} на графах большой размерности может потребовать значительных ресурсов. Однако, поскольку предложенная методология ориентирована в первую очередь на ретроспективную верификацию уже выделенного инцидента, а не на потоковый анализ, допустимо использование ресурсоёмких алгоритмов при условии распараллеливания вычислений. Инженерная оптимизация модели для работы в масштабе корпоративных SOC планируется в дальнейших исследованиях.

6.3. Место методологии в системе доказывания. Предлагаемая методология соотносится с требованиями уголовно-процессуального законодательства (ст. 86–88 УПК РФ) в части собирания, проверки и оценки доказательств:

♦ Установление причинной связи. Действующее законодательство (ст. 272.х–274.х УК РФ) требует доказывать, что ущерб наступил *именно вследствие* действий обвиняемого. Предложенный математический аппарат расчёта K_{Link} позволяет формализовать это требование, восстанавливая цепочку «Намерение – Действие – Результат».

♦ Преодоление семантического разрыва. Суды часто возвращают дела из-за того, что *технические данные не переведены на язык доказательств*. Методология обеспечивает автоматическую проекцию технических тактик на юридические признаки состава преступления, повышая научную обоснованность выводов и сокращая сроки производства экспертиз.

Экспериментальные расчёты показывают, что даже при полном устранении энтропии среды ($E_{sys} = 0$) доверие к гипотезе в рассматриваемом примере (Сценарий Б) достигает лишь значения 0.895, не пересекая порог категорического вывода $T_{verif} = 0.95$. Это не свидетельствует о слабости модели, а, напротив, отражает фундаментальное свойство доказательственного права: в условиях уголовного судопроизводства для признания факта установленным «вне разумных сомнений» недостаточно просто идеальной сохранности данных; требуется, чтобы сами доказательства (в терминах модели – W_{match} и K_{Link}) были практически безупречны (что указано в комментариях модели при вычислении K_{Link} в табл. 1). Данный результат наглядно подтверждает корректность выбранной параметризации: модель не даёт категорического заключения при недостаточной совокупной силе доказательств, даже если среда не оказывает противодействия, что отражает стандарт «вне разумных сомнений». Именно установление этой связности и устранение неоднозначности и составляет поле, на котором эксперт применяет свои профессиональные навыки: формулирует и проверяет гипотезы о способе совершения деяния, верифицирует хронологию, исключает альтернативные сценарии. Модель же предоставляет математический аппарат, переводящий результаты этой экспертной работы в формально вычислимую и процессуально значимую оценку достоверности без возможности обойти требования полноты и причинности.

Заключение. В работе сформулированы теоретические основы нового научного направления – вычислительной форензики, целью которого является разрешение фундаментального противоречия между эвристической природой традиционных экспертных методик и требованием строгой математической доказательности юридических фактов. Статья имеет постановочный характер и создаёт концептуальный каркас, на который будут опираться последующие экспериментальные работы автора.

Основные научные результаты:

1. Смена парадигмы доказывания. Обоснована необходимость перехода от парадигмы «поиска артефактов» к парадигме «формальной верификации гипотез». Как показано в исследованиях, традиционный подход, зависящий от субъективной интуиции эксперта, становится неэффективным в условиях роста объёмов данных и применения методов антифорензики. Предложенный метод заменяет субъективное «внутреннее убеждение» на объективную метрику доверия $Trust(H)$, вычисляемую на основе энтропии и каузальных связей.
2. Преодоление семантического разрыва. На основе онтологического анализа разработана формальная модель инцидента, базирующаяся на триаде «Субъект – Способ – Объект» ($S - M - O$). Доказано, что данная структура позволяет проецировать дискретные технические события (TTPs) на абстрактные юридические признаки составов преступлений (ст. 272–274 УК РФ). Это решает проблему интерпретации, когда наличие технического события (например, шифрования) не всегда очевидно означает наличие состава преступления без доказательства умысла и причинности.
3. Математизация оценки достоверности. Впервые введена модель оценки качества экспертного вывода, основанная на критериях структурной полноты, каузальной связности (K_{Link}) и штрафа за энтропию среды. Предложенный математический аппарат позволяет трансформировать задачу судебной экспертизы в класс корректных задач с вычисляемой мерой погрешности, что соответствует современным требованиям к стандартизации цифровых доказательств.

Результаты работы восполняют отмеченный в ходе анализа литературы дефицит формальных методов количественной оценки доказательственной силы, создавая теоретический базис для дальнейших исследований в области вычислительной форензики.

Разработанный концептуальный аппарат создаёт базис для проектирования интеллектуальных систем поддержки принятия решений нового поколения, способных не только выявлять инциденты, но и формировать математическое обоснование их юридической квалификации.

Дальнейшие исследования автора будут сосредоточены на:

♦ Детализации онтологии: Разработке полных онтологических карт, связывающих техники матриц MITRE ATT&CK с диспозициями статей Уголовного кодекса РФ.

♦ Математике причинности: Формализации алгоритмов расчёта коэффициента K_{Link} с использованием аппарата байесовских сетей доверия и темпоральной логики для работы с разорванными цепочками событий.

♦ Экспериментальной валидации: Апробации метода на реальных наборах данных сложных целевых атак для калибровки весовых коэффициентов модели.

Таким образом, внедрение принципов вычислительной форензики является необходимым этапом эволюции института судебной экспертизы, обеспечивающим переход от экспертного мнения к математически верифицируемому доказательству.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Sunde N., Horsman G.* The challenges and complexities of digital forensics // Forensic Science International: Digital Investigation. – 2021. – Vol. 36. – P. 301116. – URL: https://doi.org/10.1016/j.fsidi.2021.301116.
2. *Hussain S.J. and others.* A Comprehensive Survey and Analysis on Multi-Domain Digital Forensic Tools, Techniques and Issues // Research Square (Preprint). – 2022. – DOI: 10.21203/rs.3.rs-1988841/v1.
3. *Мещеряков В.А.* Теоретические основы механизма следообразования в цифровой криминалистике: монография. – М.: Проспект, 2022. – 176 с. – ISBN 978-5-392-36806-8. (дата обращения: 03.02.2026).
4. *Бессонов А.А.* Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. – 2020. – № 4 (13). – С. 13-18.
5. *Россинская Е.Р.* Теория и практика судебной экспертизы в условиях цифровизации: проблемы и перспективы // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2019. – № 5 (57). – С. 15-28.
6. *Franke K., Srihari S.N.* Computational Forensics: An Overview // Computational Forensics. IWCF 2008. Lecture Notes in Computer Science. – Berlin, Heidelberg: Springer, 2008. – Vol. 5158. – P. 1-16.
7. *Arif T., Camacho D., Park J.H.* Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security // Journal of Network and Computer Applications. – 2025. – P. 104296.
8. *Karampidis K.* A Survey on Big Data and Machine Learning in Digital Forensics // IEEE Access. – 2021. – Vol. 9. – P. 114407-114425.
9. *Amrollahi M.* Machine Learning in Digital Forensics: A Systematic Literature Review // arXiv preprint arXiv:2306.04965. – 2023.
10. *Kavrestad J., Nalle M.* Automating Digital Forensic Investigations: The Impact of Machine Learning on Electronic Evidence // 2025 IEEE International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB). – IEEE, 2025. – P. 88-93. – DOI: 10.1109/ ECAI65401.2025.11095588.
11. *Breitinger F., Baggili I.* Leveraging LLMs for Memory Forensics: A Comparative Analysis of Malware Detection // Proceedings of the 2025 ACM Asia Conference on Computer and Communications Security. – 2025. – DOI: 10.1145/3748263.
12. *Rizzo S., Bergadano F.* Explainable AI for Digital Forensics: A Review // IEEE Access. – 2024. – Vol. 12. – P. 15430-15452. – URL: https://doi.org/10.1109/ACCESS.2024.3358054.
13. *Кудрявцева А.В., Кириллова Н.П., Кочемировский В.А., Стойко Н.Г., Пристансков В.Д.* Оценка вероятностных выводов экспертов в уголовном процессе // Журнал Сибирского федерального университетата. Гуманитарные науки. – 2024. – 17 (1). – С. 4-11. – EDN: AQVACN.
14. *Руденкова Ю.С., Хазиев Ш.Н., Усов А.И.* Искусственный интеллект и судебная компьютерно-техническая экспертиза // Теория и практика судебной экспертизы. – 2024. – 19 (2). – С. 76-87. – https://doi.org/10.30764/1819-2785-2024-2-76-87.
15. *Meester R., Slooten K.* Probability and Forensic Evidence: Theory, Philosophy, and Applications. – Cambridge: Cambridge University Press, 2021. – 442 p. – DOI: 10.1017/9781108596176.
16. *Taylor D., Kokshoorn B., Champod C.* A practical treatment of sensitivity analyses in activity level evaluations // Forensic Science International. – 2024. – Vol. 355. – Article 111944. – DOI: 10.1016/j.forsciint.2024.111944.
17. *Gruber J., Humml M., Schröder L., Freiling F.* Formal Verification of Necessary and Sufficient Evidence in Forensic Event Reconstruction // Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU 2023) / eds. E. Bajramovic, R. J. Rodríguez. – Bonn, 2023. – P. 1-11.
18. *Gruber J., Humml M.* A Formal Treatment of Expressiveness and Relevance of Digital Evidence // Digital Threats: Research and Practice. – 2023. – DOI: 10.1145.
19. *Morgenstern M., Fähndrich J., Honekamp W.* Ontology in the Digital Forensics Domain: A Scoping Review // INFORMATIK 2022. – Bonn: Gesellschaft für Informatik, 2022. – P. 71-80. – URL: https://doi.org/10.18420/inf2022_07.
20. *Silva T.J., Oliveira Jr E., Zorzo A.F.* How Ontologies Have Supported Digital Forensics: Review and Recommendations // Forensic Science Review. – 2024. – Vol. 36, No. 2. – P. 99-125.

21. *Li S.* Blockchain-based digital forensic evidence traceability framework // Computers & Security. – 2022. – Vol. 115. – P. 102604. – URL: https://doi.org/10.1016/j.cose.2022.102604.
22. *Крюков Р.О., Федорченко Е.В., Котенко И.В. [и др.].* Оценка защищённости на основе графов атак с использованием базы данных NVD и MITRE ATT&CK для гетерогенных инфраструктур // Информационно-управляющие системы. – 2024. – № 2. – С. 39-50. – URL: https://doi.org/10.31799/1684-8853-2024-2-39-50.
23. *Angelini M.* PERCIVAL: Proactive and rEactive attack and Response assessmenT for Cyber Incidents Using Visual AnaLytics // IEEE Symposium on Visualization for Cyber Security (VizSec). – 2021. – P. 1-11. – URL: https://doi.org/10.1109/VizSec53982.2021.9645938.
24. *Lallie C.G.* A review of attack graph and attack tree visual syntax in cyber security // Computer Science Review. – 2021. – Vol. 39. – P. 100346. – URL: https://doi.org/10.1016/j.cosrev.2020.100346.
25. *Uddin M.* A survey of attack graph-based security analysis and network hardening // Computers & Security. – 2023. – Vol. 128. – P. 103157. – URL: https://doi.org/10.1016/j.cose.2023.103157.
26. *Marrara S.* Legal and Ethical Challenges in Digital Forensics Investigations // Digital Forensics and Cyber Crime. – IGI Global, 2024. – P. 112-135. – URL: https://scholar.google.com/scholar?q=Legal+and+Ethical+Challenges+in+Digital+Forensics+Investigations.
27. *Horsman G.* Frameworks for digital forensic evidence presentation // Forensic Science International: Digital Investigation. – 2021. – Vol. 38. – P. 301124. – URL: https://doi.org/10.1016/ j.fsidi.2021.301124.
28. *Геворгян Р.А., Абрамов Е.С.* Онтологический подход к формализации модели компьютерного инцидента и методу идентификации его структурных элементов в задачах судебной экспертизы. – https://doi.org/10.5281/zenodo.20187983.
29. *Геворгян Р.А. Абрамов Е.С.* Анализ структурно-функциональной связи компьютерных инцидентов и типов преступлений в сфере информационной безопасности. – https://doi.org/10.5281/zenodo.20187818.
30. *Леонов А.С., Шарапов И.В.* Выбор параметра регуляризации Тихонова в некорректных задачах // Журнал вычислительной математики и математической физики. – 2021. – Т. 61, № 4. – С. 451-466. – URL: https://doi.org/10.31857/S004446692104008X.
31. *Montasari R.* A Standardised Digital Forensic Investigation Process Model (SDFIPM) // International Journal of Information Security. – 2021. – Vol. 20, No. 2. – P. 195-211. – URL: https://doi.org/10.1007/s10207-020-00495-2.
32. *Alqahtani A., Sheldon F.T.* A Survey of Formal Methods and Their Applications in Cyber Security // IEEE Access. – 2022. – Vol. 10. – P. 68702-68719. – URL: https://doi.org/10.1109/ACCESS.2022.3186256.
33. *Kaddour J.* Causal Machine Learning: A Survey and Open Problems // arXiv preprint. – 2022. – URL: https://doi.org/10.48550/arXiv.2206.15475.
34. *Lande D.* Adjustment of the analytic hierarchy process indicators using AI tools // Information Technologies and Computer Engineering. – 2025. – Vol. 22, No. 1. – P. 104-112.
35. *Sundaramoorthy S.* Cognitive bias in digital forensics: A review // Forensic Science International: Digital Investigation. – 2021. – Vol. 38. – P. 301138. – URL: https://doi.org/10.1016/j.fsidi.2021.301138.
36. *Матвеева В.С.* Статистический метод обнаружения локальных неоднородностей данных для расследования инцидентов информационной безопасности: дис. … канд. техн. наук: 05.13.19. НИЯУ МИФИ. – М., 2015.
37. *Siboni S., & Cohen A.* Anomaly Detection for Individual Sequences with Applications in Identifying Malicious Tools // Entropy. – 2020. – 22 (6), 649. – https://doi.org/10.3390/e22060649.
38. *Kim Juhwan & Son Baehoon & Yu Jihyeon & Yun Joobeom.* AI-Driven Prioritization and Filtering of Windows Artifacts for Enhanced Digital Forensics // Computers, Materials & Continua. – 2024. – 81. – P. 3371-3393. – 10.32604/cmc.2024.057234.

REFERENCES

1. *Sunde N., Horsman G.* The challenges and complexities of digital forensics, *Forensic Science International: Digital Investigation*, 2021, Vol. 36, pp. 301116. Available at: https://doi.org/10.1016/j.fsidi.2021.301116.
2. *Hussain S.J. and others.* A Comprehensive Survey and Analysis on Multi-Domain Digital Forensic Tools, Techniques and Issues, *Research Square (Preprint)*, 2022. DOI: 10.21203/rs.3.rs-1988841/v1.
3. *Meshcheryakov V.A.* Teoreticheskie osnovy mekhanizma sledoobrazovaniya v tsifrovoy kriminalistike: monografiya [Theoretical foundations of the trace formation mechanism in digital forensics: monograph]. Moscow: Prospekt, 2022, 176 p. ISBN 978-5-392-36806-8 (accessed 03 February 2026).
4. *Bessonov A.A.* Tsifrovaya kriminalisticheskaya model' prestupleniya kak osnova protivodeystviya kiberprestupnosti [Digital forensic model of a crime as a basis for countering cybercrime], *Akademicheskaya mysl'* [Academic Thought], 2020, No. 4 (13), pp. 13-18.
5. *Rossinskaya E.R.* Teoriya i praktika sudebnoy ekspertizy v usloviyakh tsifrovizatsii: problemy i perspektivy [Theory and practice of forensic examination in the context of digitalization: problems and prospects], Vestnik Universiteta imeni O.E. Kutafina (MGYUA) [Courier of the Kutafin Moscow State Law University (MSAL)], 2019, No. 5 (57), pp. 15-28.
6. *Franke K., Srihari S.N.* Computational Forensics: An Overview, *Computational Forensics. IWCF 2008. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 2008, Vol. 5158, pp. 1-16.

7. *Arif T., Camacho D., Park J.H.* Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security, *Journal of Network and Computer Applications*, 2025, pp. 104296.
8. *Karampidis K.* A Survey on Big Data and Machine Learning in Digital Forensics, *IEEE Access*, 2021, Vol. 9, pp. 114407-114425.
9. *Amrollahi M.* Machine Learning in Digital Forensics: A Systematic Literature Review, *arXiv preprint arXiv:2306.04965*, 2023.
10. *Kavrestad J., Nalle M.* Automating Digital Forensic Investigations: The Impact of Machine Learning on Electronic Evidence, *2025 IEEE International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*. IEEE, 2025, pp. 88-93. DOI: 10.1109/ECAI65401.2025.11095588.
11. *Breitinger F., Baggili I.* Leveraging LLMs for Memory Forensics: A Comparative Analysis of Malware Detection, *Proceedings of the 2025 ACM Asia Conference on Computer and Communications Security*, 2025. DOI: 10.1145/3748263.
12. *Rizzo S., Bergadano F.* Explainable AI for Digital Forensics: A Review, *IEEE Access*, 2024, Vol. 12, pp. 15430-15452. Available at: https://doi.org/10.1109/ACCESS.2024.3358054.
13. *Kudryavtseva A.V., Kirillova N.P., Kochemirovskiy V.A., Stoyko N.G., Pristanskov V.D.* Otsenka veroyatnostnykh vyvodov ekspertov v ugolovnom protsesse [Assessment of probabilistic conclusions of experts in criminal proceedings], *Zhurnal Sibirskogo federal'nogo universitetata. Gumanitarnye nauki* [Journal of Siberian Federal University. Humanities & Social Sciences], 2024, 17 (1), pp. 4-11. EDN: AQVACN.
14. *Rudenkova Yu.S., Khaziev Sh.N., Usov A.I.* Iskusstvennyy intellekt i sudebnaya komp'yuterno-tekhnicheskaya ekspertiza [Artificial intelligence and digital forensics], *Teoriya i praktika sudebnoy ekspertizy* [Theory and Practice of Forensic Science], 2024, 19 (2), pp. 76-87. Available at: https://doi.org/10.30764/1819-2785-2024-2-76-87.
15. *Meester R., Slooten K.* Probability and Forensic Evidence: Theory, Philosophy, and Applications. Cambridge: Cambridge University Press, 2021, 442 p. DOI: 10.1017/9781108596176.
16. *Taylor D., Kokshoorn B., Champod C*. A practical treatment of sensitivity analyses in activity level evaluations, *Forensic Science International*, 2024, Vol. 355, Article 111944. DOI: 10.1016/j.forsciint.2024.111944.
17. *Gruber J., Humml M., Schröder L., Freiling F.* Formal Verification of Necessary and Sufficient Evidence in Forensic Event Reconstruction, *Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU 2023)*, eds. E. Bajramovic, R. J. Rodríguez. Bonn, 2023, pp. 1-11.
18. *Gruber J., Humml M.* A Formal Treatment of Expressiveness and Relevance of Digital Evidence, *Digital Threats: Research and Practice*, 2023. DOI: 10.1145.
19. *Morgenstern M., Fähndrich J., Honekamp W.* Ontology in the Digital Forensics Domain: A Scoping Review, *INFORMATIK 2022*. Bonn: Gesellschaft für Informatik, 2022, pp. 71-80. Available at: https://doi.org/10.18420/inf2022_07.
20. *Silva T.J., Oliveira Jr E., Zorzo A.F*. How Ontologies Have Supported Digital Forensics: Review and Recommendations, *Forensic Science Review*, 2024, Vol. 36, No. 2, pp. 99-125.
21. *Li S.* Blockchain-based digital forensic evidence traceability framework, *Computers & Security*, 2022, Vol. 115, pp. 102604. Available at: https://doi.org/10.1016/j.cose.2022.102604.
22. *Kryukov R.O., Fedorchenko E.V., Kotenko I.V. [i dr.]*. Otsenka zashchishchennosti na osnove grafov atak s ispol'zovaniem bazy dannykh NVD i MITRE ATT&CK dlya geterogennykh infrastruktur [Security assessment based on attack graphs using NVD and MITRE ATT&CK databases for heterogeneous infrastructures], *Informatsionno-upravlyayushchie sistemy* [Information and Control Systems], 2024, No. 2, pp. 39-50. Available at: https://doi.org/10.31799/1684-8853-2024-2-39-50.
23. *Angelini M.* PERCIVAL: Proactive and rEactive attack and Response assessmenT for Cyber Incidents Using Visual AnaLytics, *IEEE Symposium on Visualization for Cyber Security (VizSec)*, 2021, pp. 1-11. Available at: https://doi.org/10.1109/VizSec53982.2021.9645938.
24. *Lallie C.G.* A review of attack graph and attack tree visual syntax in cyber security, *Computer Science Review*, 2021, Vol. 39, pp. 100346. Available at: https://doi.org/10.1016/j.cosrev.2020.100346.
25. *Uddin M.* A survey of attack graph-based security analysis and network hardening, *Computers & Security*, 2023, Vol. 128, pp. 103157. Available at: https://doi.org/10.1016/j.cose.2023.103157.
26. *Marrara S.* Legal and Ethical Challenges in Digital Forensics Investigations, *Digital Forensics and Cyber Crime*. IGI Global, 2024, pp. 112-135. Available at: https://scholar.google.com/scholar?q=Legal+and+Ethical+Challenges+in+Digital+Forensics+Investigations.
27. *Horsman G.* Frameworks for digital forensic evidence presentation, *Forensic Science International: Digital Investigation*, 2021, Vol. 38, pp. 301124. Available at: https://doi.org/10.1016/ j.fsidi.2021.301124.
28. *Gevorgyan R.A., Abramov E.S.* Ontologicheskiy podkhod k formalizatsii modeli komp'yuternogo intsidenta i metodu identifikatsii ego strukturnykh elementov v zadachakh sudebnoy ekspertizy [An ontological approach to formalizing a computer incident model and a method for identifying its structural elements in digital forensics]. Available at: https://doi.org/10.5281/zenodo.20187983.
29. *Gevorgyan R.A. Abramov E.S.* Analiz strukturno-funktsional'noy svyazi komp'yuternykh intsidentov i tipov prestupleniy v sfere informatsionnoy bezopasnosti. – https://doi.org/10.5281/zenodo.20187818.

30. *Leonov A.S., Sharapov I.V.* Vybor parametra regulyarizatsii Tikhonova v nekorrektnykh zadachakh, *Zhurnal vychislitel'noy matematiki i matematicheskoy fiziki*, 2021, Vol. 61, No. 4, pp. 451-466. Available at: https://doi.org/10.31857/S004446692104008X.
31. *Montasari R.* A Standardised Digital Forensic Investigation Process Model (SDFIPM), *International Journal of Information Security*, 2021, Vol. 20, No. 2, pp. 195-211. Available at: https://doi.org/10.1007/s10207-020-00495-2.
32. *Alqahtani A., Sheldon F.T.* A Survey of Formal Methods and Their Applications in Cyber Security, *IEEE Access*, 2022, Vol. 10, pp. 68702-68719. Available at: https://doi.org/10.1109/ACCESS.2022.3186256.
33. *Kaddour J.* Causal Machine Learning: A Survey and Open Problems, *arXiv preprint*, 2022. Available at: https://doi.org/10.48550/arXiv.2206.15475.
34. *Lande D.* Adjustment of the analytic hierarchy process indicators using AI tools, *Information Technologies and Computer Engineering*, 2025, Vol. 22, No. 1, pp. 104-112.
35. *Sundaramoorthy S.* Cognitive bias in digital forensics: A review, *Forensic Science International: Digital Investigation*, 2021, Vol. 38, pp. 301138. Available at: https://doi.org/10.1016/ j.fsidi.2021.301138.
36. *Matveeva V.S.* Statisticheskiy metod obnaruzheniya lokal'nykh neodnorodnostey dannykh dlya rassledovaniya intsidentov informatsionnoy bezopasnosti: dis. … kand. tekhn. nauk [Statistical method for detecting local data inhomogeneities for information security incident investigation: Cand. of eng. sc. diss.]: 05.13.19. NIYaU MIFI. Moscow, 2015.
37. *Siboni S., & Cohen A.* Anomaly Detection for Individual Sequences with Applications in Identifying Malicious Tools, *Entropy*, 2020, 22 (6), 649. Available at: https://doi.org/10.3390/e22060649.
38. *Kim Juhwan & Son Baehoon & Yu Jihyeon & Yun Joobeom.* AI-Driven Prioritization and Filtering of Windows Artifacts for Enhanced Digital Forensics, *Computers, Materials & Continua*, 2024, 81, pp. 3371-3393. 10.32604/cmc.2024.057234.

Абрамов Евгений Сергеевич – Южный федеральный университет; e-mail: abramoves@sfedu.ru; г. Таганрог, Россия; тел.: +78634371905; к.т.н.; доцент.

Abramov Eugine Sergeevich – Southern Federal University; e-mail: abramoves@sfedu.ru; Taganrog, Russia; phone: +78634371905; cand. of eng. sc.; associate professor.

УДК 004.056 DOI 10.18522/2311-3103-2026-3-68-83

М.А. Киселев

СЦЕНАРНО- И РИСК-ВЗВЕШЕННАЯ МЕТОДИКА ДЕФИЦИТА ЛОГИРОВАНИЯ ДЛЯ SIEM С ВЕРОЯТНОСТНЫМ ОПОРНЫМ ПРОФИЛЕМ ИНТЕНСИВНОСТИ И ОЦЕНКОЙ ПРИГОДНОСТИ СОБЫТИЙ К КОРРЕЛЯЦИИ

Актуальность. *Эффективность корреляции в SIEM определяется не только полнотой поступления событий, но и их пригодностью к сценарному анализу. Практические дефекты логирования, включая недологирование, нарушение временной валидности, потерю корреляционно-значимых атрибутов, снижают качество детектирования и повышают вероятность ложных срабатываний.* ***Цель.*** *Разработать сценарно- и риск-взвешенную методику количественной оценки дефицита логирования как меры пригодности потока событий к корреляции.* ***Задачи.*** *Сформировать сценарно-обоснованное множество контролируемых классов событий, задать их риск-веса, построить вероятностный опорный профиль интенсивности, ввести критерии временной валидности и структурной пригодности записи, а также получить итоговый показатель с диагностической интерпретацией причин ухудшения качества логирования.* ***Методы.*** *Использованы сценарный анализ детект-контента, риск-взвешенная агрегация, построение baseline по историческим данным, контроль временной валидности событий и оценка полноты минимально достаточных профилей корреляционно-значимых атрибутов.* ***Результаты.*** *Предложенная методика расширяет базовый показатель дефицита логирования за счёт использования вероятностного опорного профиля интенсивности, учёта перелогирования и потери корреляционно-значимых атрибутов, а также введения диагностической декомпозиции причин деградации качества логирования. Экспериментальная апробация показала, что в baseline-режиме* $DL_{new} = 0{,}000$ *при* $DL_{old} = 0{,}297$*, что подтверждает отсутствие ложных срабатываний нового показателя на штатный поток; в сценарии дублирования* $DL_{old} = 0{,}000$ *при* $DL_{new} = 0{,}073$*, что демонстрирует способность нового показателя выявлять перелогирование, невидимое для базового показателя; при нарушении временной согласованности все показатели достигают 1{,}000, что соответствует полной непригодности потока к корреляции.* ***Выводы и значимость****. Научная новизна состоит в формализации дефицита логирования как дефицита пригодности событийного потока к корреляции с учётом сценарной значимости классов событий и введении диагностической декомпози-*