Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/55-226**
Ссылка для цитирования этой статьи:
Кондратов Д.В., Володин Д.Н. // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2026. №1

УДК 51-7 DOI:10.24412/2541-9269-2026-1-3-7

ИНТЕГРАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ АНАЛИЗА РИСКОВ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Д.Н. Володин[1], Д.В. Кондратов[2]
[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов.
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов.
[1]danil3000200@mail.ru, [2]kondratovdv@yandex.ru

INTEGRATION OF MATHEMATICAL RISK ANALYSIS MODELS AND MACHINE LEARNING METHODS IN INFORMATION SECURITY MANAGEMENT SYSTEMS

D.N. Volodin[1], D.V. Kondratov[2]
[1]Saratov State Technical University named after Yuri A. Gagarin, Russia, Saratov.
[2]Saratov State Technical University named after Yuri A. Gagarin, Russia, Saratov.
[1]danil3000200@mail.ru, [2]kondratovdv@yandex.ru

Аннотация. В статье предложен подход к объединению классических математических моделей анализа рисков информационной безопасности и методов машинного обучения в рамках СУИБ. Показано, что традиционные методологии (OCTAVE, NIST SP 800-30, ISO/IEC 27005, FAIR, Монте-Карло) обеспечивают воспроизводимость и интерпретируемость оценок, но слабо учитывают динамику угроз и контекстные факторы. Методы машинного обучения позволяют выявлять скрытые закономерности, оценивать вероятности инцидентов и прогнозировать эскалацию событий по телеметрии безопасности (логи, события SIEM/EDR, сетевые потоки). Предложена архитектура гибридной модели, в которой ML-компоненты оценивают параметры (вероятность/частоту, ущерб/влияние, эффективность контролей), а математическая часть обеспечивает формальную агрегацию и управленческую интерпретацию результата. Приведены формулы, схемы и рекомендации по внедрению.

Ключевые слова: информационная безопасность, управление рисками, математические модели, машинное обучение, гибридные модели, SIEM, прогнозирование инцидентов.

Abstract. The article proposes an approach to combining classical mathematical information security risk analysis models with machine learning methods within ISMS. Traditional methodologies

(OCTAVE, NIST SP 800-30, ISO/IEC 27005, FAIR, Monte Carlo) provide reproducibility and interpretability but often fail to capture dynamic threat evolution and contextual factors. Machine learning enables discovering hidden patterns, estimating incident probabilities, and forecasting escalation based on security telemetry (logs, SIEM/EDR events, network flows). A hybrid model architecture is proposed where ML components estimate key parameters (probability/frequency, impact, control effectiveness), while the mathematical layer provides formal aggregation and managerial interpretation. Formulas, block diagrams, and practical implementation recommendations are provided.

Keywords: information security, risk management, mathematical models, machine learning, hybrid models, SIEM, incident forecasting.

Современная организация редко обладает статичной ИТ-средой. В процессе цифровой трансформации постоянно появляются новые сервисы, меняются сетевые периметры, возрастает доля облачных технологий, расширяются интеграционные взаимодействия и уровень автоматизации бизнес-процессов. Параллельно с этим эволюционируют и угрозы информационной безопасности: злоумышленники активно используют многоэтапные фишинговые цепочки, техники living-off-the-land, эксплуатацию уязвимостей цепочек поставок, компрометацию учётных записей и злоупотребление программными интерфейсами (API). В результате риск информационной безопасности становится сложной функцией времени, контекста и поведения пользователей и систем.

Классические подходы к анализу рисков информационной безопасности обладают рядом существенных преимуществ. Они формализуют процесс управления рисками, включая этапы идентификации, оценки, обработки и мониторинга, обеспечивают связь технических мер защиты с целями бизнеса и требованиями комплаенса, а также позволяют получать интерпретируемые и проверяемые результаты, пригодные для аудита и управленческих решений. Однако на практике данные подходы часто опираются на экспертные шкалы качественной оценки, усреднённые вероятности наступления инцидентов и редко обновляемые реестры рисков, что снижает их точность в условиях динамично меняющегося ландшафта угроз.

Методы машинного обучения частично компенсируют указанные ограничения за счёт анализа реальных событий информационной безопасности, выявления скрытых закономерностей в телеметрии и построения прогнозов вероятности инцидентов. Такие методы способны адаптироваться к изменениям среды и учитывать поведенческие и контекстные факторы, что делает их перспективным инструментом для поддержки принятия решений в системах управления информационной безопасностью. Целью данной статьи является описание практической модели интеграции математических методов анализа рисков и подходов машинного обучения в рамках СУИБ с сохранением интерпретируемости и управляемости результатов.

В информационной безопасности риск традиционно рассматривается как сочетание вероятности реализации нежелательного события и величины ущерба,

который это событие может нанести активам организации. Под активами понимаются данные, информационные системы, сервисы, инфраструктурные компоненты и бизнес-процессы, обладающие ценностью. Угроза представляет собой потенциальный источник вреда, уязвимость — слабое место системы, повышающее вероятность реализации угрозы, а контроли предназначены для снижения вероятности инцидента либо уменьшения его последствий.

Наиболее распространённой формой количественной оценки риска является выражение $R = P * I$, где где R — риск, P — вероятность или частота инцидента, I — величина ущерба. Для учёта уязвимостей и мер защиты используется расширенная модель $R = P(T) * V * I\ (1 - E_C)$, где V характеризует степень уязвимости, а E_C — эффективность контролей.

В факторных моделях риск интерпретируется как математическое ожидание потерь за период времени и может быть записан в виде $R = E[Loss] = \lambda * E[L]$, где $\lambda -$ интенсивность возникновения инцидентов, а L — случайная величина ущерба. Такое представление удобно для интеграции с методами машинного обучения, поскольку параметры модели могут оцениваться на основе фактических данных.

Несмотря на методологическую проработанность, классические модели анализа рисков обладают рядом ограничений. В рекомендациях NIST и стандартах ISO/IEC значительная часть параметров определяется экспертным путём, что вносит субъективность и снижает оперативность обновления оценок. Методологии, ориентированные на организационный контекст, такие как OCTAVE, требуют значительных ресурсов и не предназначены для частого пересмотра рисков. Имитационные методы, включая моделирование Монте-Карло, позволяют учитывать неопределённость, но зависят от качества исходных распределений.

Общей проблемой указанных подходов является их ограниченная способность учитывать динамику угроз, поведенческие особенности пользователей и эволюцию атакующих техник, что особенно критично в условиях современных целевых атак.

Методы машинного обучения позволяют анализировать телеметрию безопасности, включающую журналы событий, сетевые потоки, данные SIEM, EDR и систем управления доступом. На основе этих данных возможно построение моделей, оценивающих вероятность и частоту инцидентов, прогнозирующих величину ущерба и анализирующих эффективность мер защиты.

В отличие от экспертных оценок, машинное обучение опирается на фактические данные и способно выявлять закономерности, неочевидные при традиционном анализе. Однако результаты работы ML-моделей зачастую обладают низкой интерпретируемостью и не могут быть напрямую использованы в управленческих процессах без дополнительной формализации.

Ключевая идея интеграции заключается в разделении ролей между компонентами гибридной системы. Машинное обучение используется для

динамической оценки параметров риска, таких как вероятность инцидента, интенсивность событий, величина ущерба и эффективность контролей. Математическая модель выступает в роли формального ядра, обеспечивающего расчёт, агрегацию и интерпретацию результатов.

В интегрированной системе машинное обучение формирует количественные оценки параметров риска на основе актуальной телеметрии безопасности. Эти оценки подаются на вход математической модели, где используются в формализованных выражениях для расчёта итоговых значений риска. Для отдельного сценария риска расчёт может быть представлен в виде $R_s(t) = \lambda_S(t) * E[L_s(t)] * (1 - E_{C,s}(t))$.

Агрегация рисков по активам и бизнес-процессам обеспечивает поддержку управленческих решений и приоритизацию мер защиты.

Особое значение интеграция приобретает на этапе мониторинга. В отличие от статического подхода гибридная модель позволяет осуществлять непрерывную актуализацию оценок по мере поступления новых данных, что обеспечивает своевременное выявление роста уровня риска.

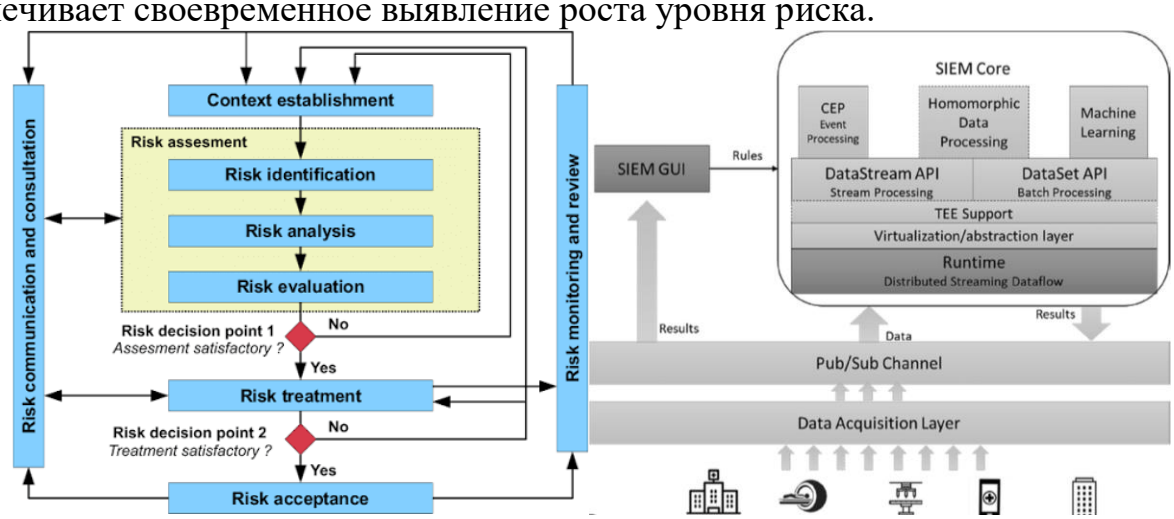

Рисунок 1 — Архитектура интеграции математических моделей анализа рисков и методов машинного обучения в СУИБ

На рисунке представлена обобщённая архитектура интегрированной системы. Источниками данных выступают средства мониторинга и защиты, формирующие телеметрию безопасности. После этапов сбора и нормализации данные используются для работы моделей машинного обучения, оценивающих параметры риска. Полученные значения передаются в математический модуль расчёта риска, обеспечивающий формализованную агрегацию и интерпретацию результатов. Итоговые оценки используются для актуализации реестра рисков и поддержки управленческих решений.

Интеграция математических моделей анализа рисков и методов машинного обучения представляет собой перспективное направление развития систем управления информационной безопасностью. Такой подход позволяет сохранить формальную строгость, интерпретируемость и соответствие стандартам, одновременно используя адаптивность и прогностические возможности

интеллектуальных методов. В условиях динамичного ландшафта угроз гибридные модели создают основу для более точного, актуального и обоснованного управления рисками информационной безопасности.

Литература

1. Первушина, Т. Л. Оценка и анализ рисков : учебное пособие / Т. Л. Первушина. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2022. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/330179 (дата обращения: 15.12.2025). — Режим доступа: для авториз. пользователей.
2. Полшков, Ю. Н. Теоретико-методологические основы и прикладные аспекты математического моделирования экономической деятельности и процессов управления регионально-отраслевым развитием : монография / Ю. Н. Полшков, А. В. Половян, М. Ю. Терентьева. — Донецк : ДонГУ, 2025. — 392 с. — ISBN 978-5-00261-168-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504617 (дата обращения: 18.12.2025). — Режим доступа: для авториз. пользователей.
3. Антюхов, В. И. Управление рисками, системный анализ и моделирование : учебное пособие / В. И. Антюхов, Г. Н. Заводсков, А. П. Корольков. — Санкт-Петербург : СПбУ ГПС МЧС России, 2024. — 256 с. — ISBN 978-5-907724-90-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/498599 (дата обращения: 17.12.2025). — Режим доступа: для авториз. пользователей.
4. Фомичева, С. Г. Методы машинного обучения в задачах обеспечения информационной безопасности : учебное пособие / С. Г. Фомичева. — Санкт-Петербург : ГУАП, 2023. — 136 с. — ISBN 978-5-8088-1822-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341024 (дата обращения: 14.12.2025). — Режим доступа: для авториз. пользователей.
5. Целых, А. Н. Принятие решений на основе методов машинного обучения : учебное пособие / А. Н. Целых, Н. В. Драгныш, Э. М. Котов. — Ростов-на-Дону : ЮФУ, 2022. — 113 с. — ISBN 978-5-9275-4246-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/345512 (дата обращения: 17.12.2025). — Режим доступа: для авториз. пользователей.