УДК 004

Гибридный подход к автоматизированному аудиту информационной безопасности на основе ИИ и требований ГОСТ Р ИСО/МЭК 27001–2021

Тютюнник Д.А. (ИТМО)

Научный руководитель – доктор технических наук, профессор Лившиц И.И. (ИТМО)

Введение. Рынок аудита информационной безопасности в России растёт: в 2025 году его объём достиг 25 млрд рублей (+25% к 2024 г.) [1]. На Россию пришлось 14–16% всех успешных кибератак в мире за период с июля 2024 по сентябрь 2025 года [2]. Особенно тревожит, что 96% компаний уязвимы к атакам через известные уязвимости с публичными эксплойтами [3], а 6 из 10 организаций имеют критические ошибки в конфигурации – слабую аутентификацию, устаревшее ПО, незащищённые веб-приложения [4]. По данным PT SWARM, при пентестах доступ к корпоративной сети получен в 89% случаев, а полный контроль над доменом – в 100% [2]. В этих условиях традиционный аудит не справляется с масштабом угроз. Возникает потребность в автоматизированных ИИ-поддерживаемых подходах, способных выявлять недостатки и генерировать превентивные рекомендации. Настоящая работа направлена на разработку такой методики.

Основная часть. Современные системы менеджмента информационной безопасности (СМИБ), построенные в соответствии с ГОСТ Р ИСО/МЭК 27001–2021, требуют регулярного аудита, однако на практике он остаётся ручным, трудоёмким и субъективным [5]. Даже при использовании сканеров уязвимостей эксперту приходится вручную интерпретировать данные и формулировать рекомендации. При этом ГОСТ Р ИСО/МЭК 27006–2020 чётко разделяет типы проверок – организационные, технические, визуальные и испытания, – но существующие инструменты редко покрывают все измерения [6].

Для решения этой проблемы предложена гибридная методика, основанная на четырёхмерной модели аудита. Для каждого из 113 контролей Приложения А ГОСТ Р ИСО/МЭК 27001–2021 система заранее хранит:

– текст требования;

– тип контроля (организационный/технический);

– допустимые типы проверок согласно ГОСТ Р ИСО/МЭК 27006–2020 («Х», «Рекомендуется», «Возможно»).

Четвёртый параметр – фактическое значение – поступает от пользователя (результаты сканирования, статус служб, наличие документов). На основе этих данных формируется структурированный запрос к крупной языковой модели (LLM), включающий требование стандарта, типы проверок и текущее состояние. Это позволяет генерировать целевые рекомендации по каждому типу проверки.

Например, для контроля А.9.4.2 «Безопасные процедуры входа в систему» при обнаружении активной учётной записи «Гость» и отсутствия МФА система выдаёт:

– организационную меру: «Утвердить Политику ИБ с требованием МФА»;

– техническую меру: «Отключить учётную запись “Гость”»;

– меру по испытанию: «Проверить невозможность входа без токена».

Аналогично для А.12.6.1 «Управление уязвимостями» при отсутствии патча KB5032190 (CVE-2024-30048) генерируются рекомендации по обновлению ПО, внедрению регламента патч-менеджмента и автоматизации проверок.

Прототип системы реализован на Python благодаря богатой экосистеме (psutil, requests) и поддержке LLM-клиентов. Архитектура включает модули сбора данных, анализа (с базой знаний по стандартам) и формирования отчётов.

Анализ применимости методики к группам контролей показывает:

– высокая автоматизация (85–95%) – для А.8, А.9, А.12, А.13 (технические меры);

– частичная (30–50%) – для A.5, A.6, A.18 (организационные документы);
– низкая (<20%) – для A.11, A.17 (физическая безопасность).

Методика обеспечивает комплексное покрытие типов проверок, соответствует логике ГОСТ Р ИСО/МЭК 27006–2020 и значительно повышает скорость и объективность аудита за счёт ИИ-поддержки.

Выводы. Предложена методика автоматизированного аудита на основе четырёхмерной модели, объединяющая сбор конфигурационных данных и ИИ-анализ для поддержки всех типов проверок по ГОСТ Р ИСО/МЭК 27006–2020. Методика обеспечивает выявление несоответствий требованиям ГОСТ Р ИСО/МЭК 27001–2021 и генерацию как корректирующих, так и превентивных рекомендаций.

Список использованных источников:

1. Аудиторы сыграют в киберзащите: [Электронный ресурс] // Коммерсантъ. URL: https://www.kommersant.ru/doc/8341509 (Дата обращения: 22.01.2026).
2. CODE RED 2026: Актуальные киберугрозы для российских организаций: [Электронный ресурс] // ptsecurity. URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (Дата обращения: 22.01.2026).
3. 96% компаний в России можно взломать с помощью старых уязвимостей, которые уже описаны в Сети: [Электронный ресурс] // cnews. URL: https://safe.cnews.ru/news/top/2024-01-26_it-infrastruktura_96_kompanij (Дата обращения: 22.01.2026).
4. Киберугрозы в 2025: почему 96% российских компаний уязвимы и что с этим делать: [Электронный ресурс] // Компьютерра. URL: https://www.computerra.ru/324014/kiberugrozy-v-2025-pochemu-96-rossijskih-kompanij-uyazvimy-i-chto-s-etim-delat/ (Дата обращения: 22.01.2026).
5. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введ. 30.11.2021. М.: Изд-во стандартов, 2021. 28 с.
6. ГОСТ Р ИСО/МЭК 27006-2020 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введ. 01.07.2021. М.: Изд-во стандартов, 2020. 42 с.