https://doi.org/10.58805/itamns.V.1(32)-11

АВТОМАТИЗАЦИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ НА СООТВЕТСТВИЕ ЕДИНЫМ ТРЕБОВАНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Адамов, **Б.А. Тынымбаев**✉

Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан
✉ *Корреспондент-автор: tynymbaevba@gmail.com*

Received: 31 July 2026
Accepted: 08 September 2026
Published: 30 September 2026
Citation: B.A.Tynymbaev, et al. « АВТОМАТИЗАЦИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ НА СООТВЕТСТВИЕ ЕДИНЫМ ТРЕБОВАНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ». Information Technologies, Automation, and Management in Natural Sciences, vol. 1, no. 32, Sept. 2026, doi: https://doi.org/10.58805/itamns.V.1(32)-11
License CC BY 4.0

Статья посвящена разработке веб-платформы автоматизации испытаний информационных систем (ИС) на соответствие Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждённым Постановлением Правительства Республики Казахстан №832. Рассматривается нормативная база проведения испытаний ИС, анализируются проблемы ручного подхода к аттестации. Предложена формализованная балловая модель оценки соответствия с целевым показателем 200 очков, включающая три типа испытаний: вопросное тестирование по группам Единых требований, нагрузочное тестирование и статический анализ кода. Описана архитектура платформы на основе стека FastAPI (Python 3.12) + React 18 (TypeScript) + PostgreSQL 16 с поддержкой мультитенантности и иерархической ролевой моделью доступа. Представлены модули классификации ИС по уровням Высокий/Средний/Низкий, моделирования угроз, совместимого со STRIDE-методологией, и цифрового плана действий с автоматической генерацией пунктов по каждому выявленному несоответствию. Проведённая апробация показала сокращение времени подготовки протокола испытаний с трёх рабочих дней до шести часов. Платформа ориентирована на организации, подпадающие под казахстанское законодательство об информатизации, в том числе объекты КВОИКИ.

Ключевые слова: испытания информационных систем, Единые требования ИБ, КВОИКИ, автоматизация аудита, вопросное тестирование, нагрузочное тестирование, анализ кода, моделирование угроз, балловая модель, платформа соответствия, Казахстан.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ БІРЫҢҒАЙ ТАЛАПТАРҒА СӘЙКЕСТІККЕ АРНАЛҒАН СЫНАҚТАРДЫ ӨТКІЗУДІ АВТОМАТТАНДЫРУ

Ә.Ә. Адамов, **Б.А. Тынымбаев**✉

Л. Н. Гумилев атындағы Еуразиялық ұлттық университеті, Астана, Қазақстан,
✉ *e-mail: tynymbaevba@gmail.com*

Мақала Қазақстан Республикасы Үкіметінің №832 қаулысымен бекітілген ақпараттық-коммуникациялық технологиялар саласындағы және ақпараттық қауіпсіздікті қамтамасыз ету бойынша Бірыңғай талаптарға ақпараттық жүйелерді (АЖ) сынаудың веб-платформасын автоматтандыруды әзірлеуге арналған. АЖ-ды сынаудың нормативтік базасы қарастырылады, аттестаттаудың қолмен орындалатын тәсілінің мәселелері талданады. 200 ұпай мақсатты көрсеткіші бар сәйкестікті бағалаудың формализацияланған ұпайлық моделі ұсынылды, ол үш сынақ түрін қамтиды: Бірыңғай талаптардың топтары бойынша сауалнамалық тестілеу, жүктемелік тестілеу және кодты статикалық талдау. Мультитенантты қолдаумен FastAPI (Python 3.12) + React 18

(TypeScript) + PostgreSQL 16 стекіне

негізделген платформа архитектурасы сипатталады. АЖ-ды Жоғары/Орта/Төмен деңгейлер бойынша жіктеу, STRIDE-методологиясымен үйлесімді қауіп модельдеу модульдері және анықталған әрбір сәйкессіздік бойынша бөлімдерді автоматты түрде генерациялайтын цифрлық іс-қимыл жоспары ұсынылған. Апробация сынақ хаттамасын дайындау уақытын үш жұмыс күнінен алты сағатқа дейін қысқартуды көрсетті.

Түйін сөздер: ақпараттық жүйелерді сынау, ИБ Бірыңғай талаптары, КМААКИ, аудитті автоматтандыру, сауалнамалық тестілеу, жүктемелік тестілеу, кодты талдау, қауіп модельдеу, ұпайлық модель, сәйкестік платформасы, Қазақстан.

AUTOMATION OF CONFORMANCE TESTING TO UNIFIED INFORMATION SECURITY REQUIREMENTS

A.A. Adamov, **B.A. Tynymbaev**✉

L. N. Gumilyov Eurasian National University, Astana, Kazakhstan,
✉*e-mail: tynymbaevba@gmail.com*

This article presents the development of a web platform for automating the conformance testing of information systems (IS) against the Unified Requirements in the field of information and communication technologies and information security, approved by Resolution №832 of the Government of the Republic of Kazakhstan. The regulatory framework for IS testing is examined, and the problems inherent in manual attestation approaches are analyzed. A formalized scoring model with a target of 200 points is proposed, incorporating three types of tests: questionnaire-based testing against Unified Requirements groups, load testing, and static code analysis. The platform architecture based on a FastAPI (Python 3.12) + React 18 (TypeScript) + PostgreSQL 16 stack with multi-tenancy support and hierarchical role-based access control is described. Modules for IS classification (High/Medium/Low levels), STRIDE-compatible threat modeling, and a digital action plan with automatic item generation for each identified non-conformance are presented. Pilot deployment demonstrated a reduction in protocol preparation time from three working days to six hours. The platform targets organizations subject to Kazakhstan's informatization legislation, including critical information and communication infrastructure (CICI) facilities.

Keywords: information system testing, unified information security requirements, CICI, audit automation, questionnaire testing, load testing, code analysis, threat modeling, scoring model, compliance platform, Kazakhstan.

Введение. Курс Казахстана на цифровую трансформацию государственного управления - программы «Цифровой Казахстан» (2018–2022) и «Цифровой Казахстан 2.0» - привёл к значительному росту числа государственных информационных систем и систем, отнесённых к критически важным объектам информационно-коммуникационной инфраструктуры (КВОИКИ). Операторы таких систем обязаны проходить испытания на соответствие Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждённым Постановлением Правительства РК № 832 [1]. Порядок и методика проведения испытаний закреплены в Приказе МЦРИАП № 111/НҚ. [2].

На практике процедура испытаний, как правило, выполняется вручную: аудитор обходит контрольные вопросы в таблицах Microsoft Excel, вносит ответы, суммирует баллы и составляет акт испытаний. Данный подход обладает рядом существенных недостатков. Во-первых, трудоёмкость: подготовка протокола для одной ИС занимает от трёх до пяти рабочих дней. Во-вторых, слабая воспроизводимость: итоговый балл зависит от квалификации конкретного специалиста и его интерпретации требований. В-третьих, отсутствие сквозного трекинга устранения несоответствий: после выдачи предписания контроль его исполнения ведётся в отдельных электронных таблицах или по электронной почте, что затрудняет верификацию при повторных испытаниях.

Мировая практика показывает, что перечисленные проблемы решаются через специализированные платформы управления соответствием (Compliance Management Platforms, CMP). Однако коммерческие решения - Vanta, Drata, Tugboat Logic - ориентиро-

ваны на международные фреймворки (SOC 2, ISO 27001) и не поддерживают казахстанскую нормативную базу [3]. Открытых публикаций об инструментах автоматизации испытаний именно по ПП № 832 нами не выявлено.

Цель настоящей работы - описать архитектуру и функциональную модель веб-платформы Audit Prep Platform, автоматизирующей проведение испытаний ИС на соответствие Единым требованиям, и оценить её практическую эффективность по результатам пилотного применения.

Материалы и методы. Нормативной основой исследования служат: Постановление Правительства РК № 832 (редакция 2022 года) [1], Приказ МЦРИАП № 434 «Об утверждении Правил проведения испытаний информационных систем» [2], Закон РК «Об информатизации» № 418-V [4], а также Правила отнесения объектов информационно-коммуникационной инфраструктуры к критически важным (Постановление Правительства РК, ноябрь 2022) [5].

В основу проектирования платформы положен метод Design Science Research [6], предполагающий итеративное создание артефакта (программной системы) с последующей его оценкой в реальных условиях. Архитектурные решения разрабатывались с применением принципов Domain-Driven Design и API-first подхода; модель угроз строилась в соответствии с методологией STRIDE [7, 8]. Сравнительный анализ существующих решений проводился методом систематического обзора публикаций в базах IEEE Xplore, ACM Digital Library и ResearchGate за период 2019–2024 годов.

Обзор литературы и существующих решений. Автоматизация ИБ-аудита и тестирования соответствия. Автоматизация процессов аудита информационной безопасности привлекает устойчивое внимание исследователей. Antunes и соавторы [3] описывают веб-платформу управления соответствием стандартам ИБ с гибкой загрузкой контрольных чеклистов; архитектура и модель данных системы были апробированы на 50 малых и средних предприятиях в рамках проекта внедрения ISO 27001:2013. Полученные результаты подтверждают применимость реляционной базы данных и веб-интерфейса для управления оценками соответствия, однако система не предусматривает поддержки национальных нормативных актов.

Ghanem и соавторы [7] предложили фреймворк ESASCF для автоматизации compliance-тестирования и пенетрационного тестирования на основе экспертных систем с возможностью извлечения, и повторного применения экспертных знаний. Работа демонстрирует, что формализация экспертизы в базе правил позволяет существенно ускорить выполнение рутинных проверок; вместе с тем создание базы знаний требует значительных первоначальных инвестиций.

Deore и Patil [8] систематизируют стратегии автоматизации тестирования безопасности, выделяя три основных класса: автоматизированное сканирование уязвимостей, инструментальное пенетрационное тестирование и автоматизация compliance-проверок. Авторы подчёркивают, что инструменты continuous compliance monitoring способны снизить риск нарушения регуляторных требований и повысить доверие аудиторов. Murat и соавторы [9] провели систематическое картирование литературы по тестированию безопасности веб-приложений и показали, что автоматизация покрывает преимущественно технические аспекты, тогда как организационные и нормативные аспекты остаются в значительной степени ручными.

Моделирование угроз. Методология STRIDE, разработанная в Microsoft и подробно описанная в монографии Shostack [10], предлагает систематическую классификацию угроз по шести категориям: спуфинг, фальсификация, отказ от авторства, раскрытие информации, отказ в обслуживании и повышение привилегий. ISACA [11] в 2024 году охарактеризовала STRIDE как наиболее зрелую и практически применимую методологию threat modeling для корпоративных ИС, рекомендовав её как отправную точку при разработке специализированных инструментов. Abdelrazek и соавторы [12] предложили подход к автоматизированному анализу рисков архитектуры ПО на основе формализованных сигнатур угроз, что подтверждает возможность алгоритмического расчёта оценок риска.

Казахстанский регуляторный контекст и gap-анализ. Казахстанское законодательство об информационной безопасности претерпело существенное обновление в 2022 году: были приняты новые Критерии отнесения объектов ИКИ к критически важным [5], расширен перечень обязательных требований ПП № 832 и уточнены правила проведения испытаний. Как отмечает Dentons [5], для большинства ИТ-компаний, работающих в Казахстане, соответствие требованиям КВОИКИ стало обязательным условием ведения деятельности. Тем не менее специализированных инструментов автоматизации испытаний именно по казахстанской нормативной базе в откры-

тых источниках не обнаружено. Это формирует значимый технологический и научный пробел, который данная работа стремится восполнить.

Существующие коммерческие CMP-платформы (Vanta, Drata, Hyperproof) ориентированы на международные фреймворки - SOC 2, ISO 27001, GDPR - и не содержат встроенной поддержки структуры Единых требований РК. Попытки адаптировать эти инструменты путём ручного создания кастомных чеклистов возможны, но требуют значительных трудозатрат и не обеспечивают автоматического расчёта балла по методике Приказа № 434.

Нормативная база испытаний информационных систем в Республике Казахстан.

Субъекты и объём обязательств. Испытания на соответствие Единым требованиям обязательны для государственных органов - операторов государственных информационных систем (ГИС), а также для владельцев и операторов объектов КВОИКИ [1, 3]. Критически важными объектами признаются ИКИ, нарушение функционирования которых может повлечь угрозу национальной безопасности, значительный экономический ущерб или нарушение конституционных прав граждан [5]. По состоянию на 2022 год к этой категории отнесены банковские и финансовые системы, объекты энергетики и транспорта, телекоммуникационная инфраструктура, а также информационные системы ряда государственных органов.

Структура Единых требований. Постановление № 832 структурирует Единые требования по нескольким группам: общие требования к информационным системам; требования к защите информации от несанкционированного доступа; требования к криптографической защите; требования к сетевой безопасности; требования к физической безопасности серверных помещений; требования к персоналу и процессам управления ИБ; требования к резервному копированию и восстановлению. Каждая группа содержит конкретные индикаторы (контрольные вопросы), по которым производится оценка соответствия ИС. Общее число обязательных контрольных вопросов для ГИС первой категории превышает 150.

Процедура испытаний по Приказу № 434. Правила проведения испытаний предусматривают последовательность из пяти этапов: (1) подача заявки оператором ИС; (2) формирование программы и методики испытаний испытательной лабораторией; (3) непосредственное проведение испытаний вопросное, инструментальное и нагрузочное; (4) оформление акта и протокола испытаний с балловой оценкой; (5) выдача аттестата соответствия либо предписания об устранении несоответствий. Целевой балл для прохождения испытаний составляет 200 очков.

Ручная реализация этой процедуры порождает ряд системных проблем, которые проиллюстрированы в таблице 1.

Таблица 1 - Сравнение ручного и автоматизированного подходов к проведению испытаний ИС

Параметр	Ручной подход	Автоматизированный подход (платформа)
Трудозатраты на одну ИС	3–5 рабочих дней	4–8 часов
Воспроизводимость результата	Зависит от квалификации аудитора	Детерминирована алгоритмом расчёта балла
Трекинг устранения несоответствий	Email-переписка / отдельные таблицы Excel	Встроенный план действий с привязкой к вопросу
Повторные испытания	Повторный ввод данных с нуля	Инкрементальное обновление; baseline из предыдущего цикла
Архив результатов	Файловый сервер (Excel/PDF)	Реляционная БД с версионированием и полным аудит-логом
Совместная работа группы аудиторов	Затруднена (конфликты версий)	Нативная поддержка ролей OWNER/ADMIN/AUDITOR/VIEWER

Результаты и обсуждение. *Архитектура платформы автоматизации. Общая схема и технологический стек.;* Платформа Audit Prep Platform построена по трёхзвенной клиент-серверной архитектуре. Клиентская часть - одностраничное приложение (SPA) на React 18 + TypeScript с использованием TanStack React Query для управления серверным состоянием и Tailwind CSS для адаптивного интер-

фейса. Серверная часть - REST API на FastAPI (Python 3.12) с асинхронным сервером Uvicorn, ORM SQLAlchemy 2.0 и валидацией данных через Pydantic v2. Хранилище данных - PostgreSQL 16. Развёртывание выполняется в Docker Compose; в продуктивном режиме трафик терминируется на Traefik с автоматическим получением TLS-сертификатов от Let's Encrypt.

Архитектура поддерживает мультитенантность: каждая организация создаёт одну или несколько «систем» (tenant); все данные каждой системы изолированы на уровне базы данных - каждая таблица содержит внешний ключ system_id, контроль которого осуществляется на уровне бизнес-логики бэкенда при каждом запросе. Межсистемная изоляция данных гарантируется требованием SEC-07 архитектурной спецификации.

Ролевая модель доступа. В платформе реализована двухуровневая иерархическая ролевая модель (RBAC). На глобальном уровне существуют роли администратора платформы (is_admin) и обычного пользователя. На уровне конкретной системы определены четыре роли с иерархией прав: OWNER → ADMIN → AUDITOR → VIEWER. Роль AUDITOR обеспечивает минимально необходимый набор прав для проведения испытаний: заполнение вопросного теста, ввод результатов нагрузочного тестирования, загрузка отчётов анализа кода и создание задач плана действий. Принцип минимальных привилегий [13] соблюдается на каждом эндпоинте API через middleware-проверку членства пользователя в системе и соответствия его роли.

Модульная структура. Платформа состоит из следующих функциональных модулей: аутентификация и авторизация (JWT + TOTP 2FA + SAML SSO); управление системами и участниками; модуль испытаний ИС (вопросное, нагрузочное, анализ кода); модуль классификации ИС; модуль моделирования угроз; модуль плана действий; аудит-лог (25 типов событий). В контексте настоящей статьи детально рассматриваются три центральных модуля: испытания ИС, классификация и моделирование угроз.

Модуль испытаний ИС: модель и алгоритм. Три типа испытаний и балловая модель. Модуль испытаний реализует три типа проверок, регламентированных Приказом № 434, и агрегирует их результаты в единый балл ИС с целевым показателем 200 очков. Распределение максимального балла по типам испытаний и используемые форматы ответов приведены в таблице 2.

Таблица 2 – Типы испытаний и их вклад в балл соответствия ИС

Тип испытания	Что оценивается	Формат ответа	Макс. вклад в итоговый балл
Вопросное тестирование	Соответствие ИС группам Единых требований ИБ	corresponding / not_applicable / not_corresponding	140 очков (70% от целевого балла)
Нагрузочное тестирование	Устойчивость ИС при пиковых нагрузках (RPS, процент ошибок)	Числовые метрики: хост, длительность, кол-во запросов, ошибок	40 очков (20% от целевого балла)
Анализ кода	Уязвимости в исходном коде по уровням критичности	Загрузка SAST-отчёта; отметка ложных срабатываний (FP)	20 очков (10% от целевого балла)

Алгоритм расчёта балла вопросного теста. Вопросный тест состоит из набора подтестов (subtests), каждый из которых соответствует отдельной группе Единых требований. Каждый вопрос i имеет весовой коэффициент W_i. Ответ фиксируется в одном из трёх состояний: «соответствует» (corresponding), «не применимо» (not_applicable) или «не соответствует» (not_corresponding). Итоговый балл вопросного теста Q рассчитывается по формуле (1):

$$Q = \frac{\sum W_i \times I[a_i = \text{corresponding}]}{\sum W_i \times I[a_i \neq \text{not_applicable}]} \times 140 \qquad (1)$$

где $I[\cdot]$ - индикаторная функция, принимающая значение 1 при истинности условия и 0 в противном случае; суммирование ведётся по всем вопросам теста. Вопросы с ответом «не применимо» исключаются как из числителя, так и из знаменателя, что позволяет корректно обрабатывать случаи, когда ряд требований объективно неприменим для конкретного типа ИС. При получении ответа «не соответствует» система автоматически формирует пункт плана действий, привязанный к данному вопросу.

Структура вопросного теста по Единым требованиям. Контрольные вопросы организованы в подтесты в соответствии со структурой ПП № 832. Примерное распределение вопросов по подтестам для ИС среднего уровня классификации приведено в таблице 3.

Нагрузочное тестирование: модель оценки. Нагрузочное тестирование в платформе реализует не автоматизированную генерацию нагрузки, а структурированный ввод результатов, полученных внешними инструментами (Apache JMeter, k6, Locust). Для каждого сеанса нагрузочного тестирования фиксируются: целевой хост, дата и время проведения, продолжительность теста (секунды), общее количество отправленных запросов и количество ошибочных ответов. На основании этих данных платформа автоматически рассчитывает производительность и класс результата. Балл нагрузочного теста определяется по порогу процента ошибок: при Error rate <1% начисляется максимальный балл; при значениях 1–5% - пропорционально сниженный; при Error rate > 5% балл равен нулю и автоматически создаётся пункт плана действий.

Таблица 3 - Структура вопросного теста по группам Единых требований (пример для ИС среднего уровня)

Группа Единых требований	Примеры контрольных вопросов	Кол-во вопросов
Управление доступом	Реализована ли двухфакторная аутентификация для привилегированных пользователей? Ведётся ли журнал всех попыток доступа с фиксацией времени, пользователя и результата?	15–20
Криптографическая защита	Применяются ли сертифицированные средства криптографической защиты информации? Обеспечено ли шифрование каналов передачи данных, содержащих конфиденциальную информацию?	10–15
Защита от несанкционированного доступа	Настроены ли межсетевые экраны и правила фильтрации трафика? Проводится ли непрерывный мониторинг сетевого трафика на предмет аномалий?	12–18
Физическая безопасность	Ограничен ли физический доступ в серверные помещения с использованием контроля доступа? Ведётся ли видеонаблюдение за серверными помещениями с хранением записей не менее 30 дней?	8–12
Управление инцидентами	Разработаны ли и актуализированы ли процедуры реагирования на инциденты ИБ? Проводятся ли регулярные учения по реагированию на инциденты с документированием результатов?	8–10
Резервное копирование и восстановление	Выполняется ли резервное копирование данных по утверждённому расписанию? Проверяется ли корректность восстановления данных из резервных копий не реже одного раза в квартал?	6–8
Управление обновлениями и уязвимостями	Установлен ли процесс своевременной установки обновлений безопасности? Проводится ли регулярное сканирование ИС на уязвимости сертифицированными инструментами?	8–10

Анализ кода: интеграция SAST-отчётов. Модуль анализа кода принимает отчёты инструментов статического анализа (SonarQube, Checkmarx, Semgrep и аналогичных) в формате CSV или JSON. Каждая уязвимость классифицируется по уровню критичности: High, Medium, Low. Аудитор имеет возможность отметить конкретные записи как ложноположительные срабатывания (is_false_positive); такие записи исключаются из расчёта итогового балла. Итоговый балл модуля кода является убывающей функцией от

взвешенного числа подтверждённых уязвимостей: каждая High-уязвимость снижает балл на 5 единиц, Medium - на 2 единицы, Low - на 0.5 единицы, но не ниже нуля.

Цифровой план действий. Одним из ключевых элементов платформы является модуль плана действий (Action Plan), обеспечивающий сквозной трекинг устранения несоответствий. Пункты плана формируются автоматически в трёх случаях: при ответе «не соответствует» в вопросном тесте; при неудовлетворительном результате нагрузочного теста; при наличии подтверждённых High-уязвимостей в отчёте анализа кода. Каждый пункт содержит описание нарушения с прямой ссылкой на конкретный вопрос или результат теста, комментарий ответственного исполнителя, статус выполнения (open / in_progress / completed) и дату закрытия. При проведении повторных испытаний пункты предыдущего цикла отображаются как исходный базис, что позволяет верифицировать факт устранения каждого несоответствия.

Модуль классификации ИС и моделирования угроз. Классификация информационных систем. Перед проведением испытаний каждая ИС проходит классификацию, определяющую объём обязательных проверок. Модуль классификации реализует иерархическую структуру параметров с весовыми коэффициентами: категории классификации → характеристики → параметры → индикаторы. Аудитор последовательно отвечает на вопросы по индикаторам; система суммирует взвешенные баллы по каждой характеристике и определяет итоговый уровень ИС: Высокий, Средний или Низкий. Данная классификация согласуется с критериями отнесения объектов ИКИ к КВОИКИ [5] и непосредственно влияет на набор подтестов в модуле испытаний: для ИС уровня «Высокий» применяется полный перечень контрольных вопросов, для «Среднего» - стандартный, для «Низкого» - сокращённый.

Моделирование угроз: STRIDE-совместимая реализация. Модуль моделирования угроз реализует подход, совместимый с методологией STRIDE [10], в части структурирования угроз по атрибутам. Для каждой ИС аудитор формирует перечень активов с оценками по трём характеристикам CIA: конфиденциальность (Confidentiality), целостность (Integrity) и доступность (Availability) — по шкале None / Low / Medium / High. На основе активов описываются угрозы, каждая из которых характеризуется вектором атаки, требуемыми привилегиями, взаимодействием с пользователем, степенью влияния на CIA и характеристиками агента угрозы (навыки, намерение, цели).

Платформа автоматически рассчитывает три производные метрики: оценку уязвимости по шкале 0-10, потенциал агента угрозы по шкале 1-18 и вероятность реализации угрозы на основе матрицы 4×4 «вероятность × влияние». Для каждой угрозы аудитор назначает одну или несколько контрмер со ссылками на соответствующие контроли CIS Controls; каждой контрмере присваивается статус: Planned / In Implementation / Implemented / Declined / Not applicable. Угрозы, для которых все контрмеры имеют статус, отличный от Implemented, автоматически включаются в дашборд остаточных рисков и могут быть перенесены в план действий для приоритизации работ.

Апробация платформы и обсуждение результатов. Пилотное применение платформы было проведено при подготовке к испытаниям двух информационных систем. ИС-1 относится к категории государственной информационной системы среднего уровня классификации (сервис документооборота организации); ИС-2 - к системам, претендующим на соответствие уровню КВОИКИ (финансовая система обработки платежей). Работы выполнялись с участием двух аудиторов, каждый из которых предварительно провёл испытания тех же систем ручным методом.

Сопоставление трудозатрат показало, что использование платформы позволило сократить время формирования протокола испытаний для ИС-1 с 3 рабочих дней до 5.5 часов, для ИС-2 - с 5 рабочих дней до 8 часов (увеличение связано с более высоким числом требований для КВОИКИ-систем). Количество выявленных несоответствий в автоматизированном режиме оказалось на 18% выше, чем при ручном методе, что объясняется стандартизированным набором вопросов платформы: аудиторы при ручном тестировании пропускали ряд подтестов как «очевидно соответствующих» без фактической проверки. Автоматически сформированный план действий содержал 23 пункта для ИС-1 и 41 пункт для ИС-2; все пункты имели прямую ссылку на конкретный нормативный вопрос, что существенно упростило работу ответственных исполнителей по устранению несоответствий.

К ограничениям проведённой апробации следует отнести: малый объём выборки (две ИС); отсутствие интеграции с инструментами автоматического сканирования уязвимостей (SAST запускался от-

дельно); а также то, что нагрузочное тестирование выполнялось внешними инструментами с последующим ручным вводом результатов в платформу.

Выводы. В настоящей работе описана архитектура и функциональная модель веб-платформы автоматизации испытаний информационных систем на соответствие Единым требованиям в области ИБ Республики Казахстан. Предложена формализованная балловая модель с целевым показателем 200 очков, охватывающая три регламентированных типа испытаний: вопросное тестирование (до 140 очков), нагрузочное тестирование (до 40 очков) и анализ кода (до 20 очков). Реализованы модули классификации ИС по уровням Высокий/Средний/Низкий, STRIDE-совместимого моделирования угроз с автоматическим расчётом оценок риска и цифрового плана действий с автогенерацией пунктов по каждому несоответствию. Результаты пилотной апробации подтвердили практическую эффективность платформы: время подготовки протокола испытаний сократилось в 3–4 раза, а полнота выявления несоответствий возросла на 18%. Платформа не имеет аналогов в открытых источниках применительно к казахстанской нормативной базе и представляет практическую ценность для ОЦИБ-лабораторий, подразделений ИБ государственных органов и операторов КВОИКИ. Направлениями дальнейшего развития являются: нативная интеграция SAST-инструментов (SonarQube, Semgrep) через API; реализация AI-ассистента для автоматической генерации рекомендаций по устранению несоответствий; поддержка формата электронного аттестата соответствия; расширение базы вопросов до полного перечня требований ПП №832 в редакции 2022 года.

Литература

1. Постановление Правительства Республики Казахстан от 20 декабря 2016 года №832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (с изменениями 2022 г.). URL: https://adilet.zan.kz/rus/docs/P1600000832 - Дата обращения: 17.12.2025.
2. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года №111/НҚ «Об утверждении методики и правил проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности». URL: https://adilet.zan.kz/rus/docs/V1900018795 - Дата обращения: 19.12.2025.
3. Antunes M., Maximiano M., Gomes R. A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing // Procedia Computer Science. - 2022. - Vol. 196. - P. 36–43. DOI 10.1016/j.procs.2021.11.070.
4. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V. URL: https://adilet.zan.kz/rus/docs/Z1500000418 - Дата обращения: 17.12.2025.
5. Dentons Kazakhstan. New Rules for IT Companies in Kazakhstan (KVOIKI Classification). - 2022. URL: https://www.dentons.com/en/insights/alerts/2022/november/29/new-rules-for-it-companies-in-kazakhstan Дата обращения: 17.12.2025.
6. Wieringa R. Design Science Methodology for Information Systems and Software Engineering. - Springer, 2014. - 332 p. ISBN 978-3-662-43838-1.
7. Ghanem M.C., Chen T.M., Ferrag M.A., Kettouche M.E. ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance // IEEE Access. - 2023. - Vol. 11. - P. 129077–129094. DOI 10.1109/ACCESS.2023.3332834.
8. Deore S., Patil A. Automating Security Testing: Strategies for Vulnerability Scanning, Penetration Testing, and Compliance Checks // International Research Journal of Engineering and Technology. - 2024. - Vol. 11(7). - P. 561–570.
9. Murat A., Cigdem A., Evren C., Alperen S. Security Testing of Web Applications: A Systematic Mapping of the Literature // Journal of King Saud University – Computer and Information Sciences. - 2022. - Vol. 34(9). - P. 6775–6792. DOI 10.1016/j.jksuci.2021.09.018.
10. Shostack A. Threat Modeling: Designing for Security. - Wiley, 2014. 480 p. ISBN 978-1-118-80999-0.
11. ISACA. Threat Modeling and Secure By Design Applications // ISACA Now Blog. - 2024. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/threat-modeling-and-secure-by-design-applications Дата обращения: 22.12.2025.

12. Abdelrazek M., Grundy J., Ibrahim A. Automated Software Architecture Security Risk Analysis Using Formalized Signatures // 2013 IEEE/ACM International Conference on Software Engineering (ICSE 2013), San Francisco. - P. 662–672. DOI 10.1109/ICSE.2013.6606612.
13. Saltzer J.H., Schroeder M.D. The Protection of Information in Computer Systems // Proceedings of the IEEE. - 1975. - Vol. 63(9). - P. 1278–1308. DOI 10.1109/PROC.1975.9939.

References

1. Postanovlenie Pravitel'stva Respubliki Kazahstan ot 20 dekabrja 2016 goda №832 «Ob utverzhdenii Edinyh trebovanij v oblasti informacionno-kommunikacionnyh tehnologij i obespechenija informacionnoj bezopasnosti» (s izmenenijami 2022 g.). URL: https://adilet.zan.kz/rus/docs/P1600000832 - Data obrashhenija: 17.12.2025. [in Russian]
2. Prikaz Ministra cifrovogo razvitija, oboronnoj i ajerokosmicheskoj promyshlennosti Respubliki Kazahstan ot 3 ijunja 2019 goda №111/NQ «Ob utverzhdenii metodiki i pravil provedenija ispytanij cifrovyh ob#ektov "cifrovogo pravitel'stva" i kriticheski vazhnyh cifrovyh ob#ektov na sootvetstvie trebovanijam kiberbezopasnosti». URL: https://adilet.zan.kz/rus/docs/V1900018795 - Data obrashhenija: 19.12.2025. [in Russian]
3. Antunes M., Maximiano M., Gomes R. A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing // Procedia Computer Science. - 2022. - Vol. 196. - P. 36–43. DOI 10.1016/j.procs.2021.11.070.
4. Zakon Respubliki Kazahstan «Ob informatizacii» ot 24 nojabrja 2015 goda №418-V. URL: https://adilet.zan.kz/rus/docs/Z1500000418 - Data obrashhenija: 17.12.2025. [in Russian]
5. Dentons Kazakhstan. New Rules for IT Companies in Kazakhstan (KVOIKI Classification). - 2022. URL: https://www.dentons.com/en/insights/alerts/2022/november/29/new-rules-for-it-companies-in-kazakhstan Data obrashenija: 17.12.2025.
6. Wieringa R. Design Science Methodology for Information Systems and Software Engineering. - Springer, 2014. - 332 p. ISBN 978-3-662-43838-1.
7. Ghanem M.C., Chen T.M., Ferrag M.A., Kettouche M.E. ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance // IEEE Access. - 2023. - Vol. 11. - P. 129077–129094. DOI 10.1109/ACCESS.2023.3332834.
8. Deore S., Patil A. Automating Security Testing: Strategies for Vulnerability Scanning, Penetration Testing, and Compliance Checks // International Research Journal of Engineering and Technology. - 2024. - Vol. 11(7). - P. 561–570.
9. Murat A., Cigdem A., Evren C., Alperen S. Security Testing of Web Applications: A Systematic Mapping of the Literature // Journal of King Saud University – Computer and Information Sciences. - 2022. - Vol. 34(9). - P. 6775–6792. DOI 10.1016/j.jksuci.2021.09.018.
10. Shostack A. Threat Modeling: Designing for Security. - Wiley, 2014. 480 p. ISBN 978-1-118-80999-0.
11. ISACA. Threat Modeling and Secure by Design Applications // ISACA Now Blog. - 2024. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/threat-modeling-and-secure-by-design-applications Data obrashenija: 22.12.2025.
12. Abdelrazek M., Grundy J., Ibrahim A. Automated Software Architecture Security Risk Analysis Using Formalized Signatures // 2013 IEEE/ACM International Conference on Software Engineering (ICSE 2013), San Francisco. - P. 662–672. DOI 10.1109/ICSE.2013.6606612.
13. Saltzer J.H., Schroeder M.D. The Protection of Information in Computer Systems // Proceedings of the IEEE. - 1975. - Vol. 63(9). - P. 1278–1308. DOI 10.1109/PROC.1975.9939.

Информация об авторах

Адамов А.А.- доктор технических наук, профессор, член-корреспондент НИА РК, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан. e-mail: adamov_aa@enu.kz;

Тынымбаев Б.А.- докторант, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан. e-mail: tynymbaevba@gmail.com.

Information about the authors

Adamov A.A.- Doctor of Technical Sciences, Professor, Corresponding Member of the NSA RK, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. e-mail: adamov_aa@enu.kz;

Tynymbaev B.A.- PhD student, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. e-mail: tynymbaevba@gmail.com.