tion Using a Hybrid Fuzzy–Simulation–ANN Model. *Applied Sciences, 16*(9). https://doi.org/10.3390/app16094364
van der Aalst W. M. P. (2016). Process Mining: Data Science in Action. Berlin ; Heidelberg: Springer. https://doi.org/10.1007/978-3-662-49851-4
Wang Y., Liao S., Gong Z., Deng F. & Yin S. (2024). Enhancing Construction Management Digital Twins Through Process Mining of Progress Logs. *Sustainability, 16*(22). https://doi.org/10.3390/su162210064

Дослідження не отримувало зовнішнього фінансування.
Автори заявляють про відсутність конфлікту інтересів.
Під час підготовки рукопису використовувався інструмент генеративного штучного інтелекту ChatGPT для формування чернеток окремих фрагментів та стилістичного редагування анотації англійською мовою. Автори несуть повну відповідальність за остаточний текст, формули, наукові положення та висновки.

Стаття надійшла до редакції / Received: 13.09.2026
Статтю прийнято до публікації / Accepted: 26.09.2026
Оприлюднено / Published: 19.10.2026

УДК 657.6:004.9:614.2
JEL: I18; M42; O33
DOI: https://doi.org/10.32983/2222-4459-2026-9-260-275

ВНУТРІШНІЙ КОНТРОЛЬ ЕЛЕКТРОННОЇ МЕДИЧНОЇ ДОКУМЕНТАЦІЇ В УМОВАХ ЦИФРОВІЗАЦІЇ ОХОРОНИ ЗДОРОВ'Я

©2026 **ГОЛОВАЧКО В. М., ГЕРИЧ М. С., ГОЛОВАЧКО А. В.**

УДК 657.6:004.9:614.2
JEL: I18; M42; O33

Головачко В. М., Герич М. С., Головачко А. В. Внутрішній контроль електронної медичної документації в умовах цифровізації охорони здоров'я

Прогалина полягає у відсутності цілісної методики, що одночасно охоплює якість даних, законність оброблення, доступ, авторство, інтероперабельність, відновлюваність і журнали подій як контрольні докази. Метою статті є теоретичне обґрунтування та розроблення ризик-орієнтованої методики внутрішнього контролю електронної медичної документації. Застосовано нормативно-документальний аналіз українських і європейських актів, структурований цільовий огляд рецензованих праць 2020–2026 рр., порівняльне зіставлення вимог ISO 27799:2025, ISO/IEC 27001:2022 та Глобальних стандартів внутрішнього аудиту, процесну декомпозицію, ризик-орієнтоване моделювання, сценарне тестування й аналіз чутливості. За результатами визначено дев'ять контрольних цілей: законність і визначена мета; правильна ідентифікація; повнота; точність і правдоподібність; своєчасність; конфіденційність і мінімально необхідний доступ; цілісність і авторство; доступність і відновлюваність; простежуваність та інтероперабельність. Розроблено матрицю для восьми ділянок життєвого циклу документації, яка пов'язує ризики з превентивними, виявляльними й коригувальними процедурами та доказами їх виконання. Запропоновано розподіл відповідальності за моделлю трьох ліній, десять кількісних індикаторів, формулу залишкового ризику та інтегральний індекс зрілості контролю з п'ятьма рівнями. Сценарне тестування дало модельне зменшення сукупного ризику зі 135 до 47,84 бала (64,56%); сценарний індекс зрілості становив 42,50% за цільового значення 80,00%. За незмінної номінальної результативності 80% зниження надійності доказу від 1,00 до 0,60 збільшує залишковий ризик із 5,00 до 13,00. Наукова новизна полягає в інтеграції нормативних і медичних вимог, вимог інформаційної безпеки та внутрішнього аудиту, а також у застосуванні коефіцієнта D для коригування результативності контролю та залишкового ризику з урахуванням надійності контрольного доказу. Практична цінність результатів визначається можливістю використання матриці як основи локального положення, програми внутрішнього аудиту, технічного завдання до медичної інформаційної системи та управлінської панелі показників. Сценарні результати демонструють узгодженість алгоритму, але не є емпіричною оцінкою ефекту; ваги, пороги та параметри потребують локальної калібрації й валідації на знеособлених даних.
Ключові слова: *внутрішній контроль; електронна медична документація; електронна система охорони здоров'я; медична інформаційна система; якість даних; аудит-лог; захист персональних даних; ризик-орієнтований підхід.*
Табл.: *9.* ***Формул:*** *6.* ***Бібл.:*** *19.*

Головачко Василь Михайлович *– кандидат економічних наук, доцент, доцент кафедри обліку і оподаткування та маркетингу, Мукачівський державний університет (вул. Ужгородська, 26, Мукачево, 89600, Україна)*
E-mail: *wasjahol1980@gmail.com*
ORCID: *https://orcid.org/0000-0002-5993-0873*

Герич Мирослава Сергіївна *– кандидат фізико-математичних наук, доцент кафедри теорії ймовірностей і математичного аналізу, Ужгородський національний університет (пл. Народна, 3, Ужгород, 88000, Україна)*
E-mail: *miroslava.gerich@uzhnu.edu.ua*
ORCID: *https://orcid.org/0000-0001-9634-5254*

Головачко Анастасія Василівна *– магістрант, Львівський національний медичний університет імені Короля Данила (вул. Пекарська, 69, Львів, 79010, Україна)*
E-mail: *anastasiagolovacko@gmail.com*
ORCID: *https://orcid.org/0009-0006-9879-9229*

UDC 657.6:004.9:614.2
JEL: I18; M42; O33

Holovachko V. M., Herych M. S., Holovachko A. V. Internal Control of Electronic Medical Documentation in the Context of Healthcare Digitalization
The research gap lies in the absence of an integrated methodology that simultaneously covers medical data quality, lawful processing, access management, authorship of electronic records, interoperability, recoverability, and the use of event logs as control evidence. The article aims to substantiate and develop a risk-based methodology for the internal control of electronic medical documentation. Methods include analysis of Ukrainian and EU acts, a structured review

of peer-reviewed studies (2020–2026), mapping against ISO 27799:2025, ISO/IEC 27001:2022, and the Global Internal Audit Standards, process decomposition, risk-based modelling, scenario testing, and sensitivity analysis. The results identify nine control objectives: lawfulness and purpose limitation; correct patient identification; completeness; accuracy and plausibility; timeliness; confidentiality and minimum-necessary access; integrity and authorship; availability and recoverability; and traceability and interoperability. A matrix is developed for eight stages of the documentation life cycle, linking risks with preventive, detective, and corrective procedures and the evidence of their performance. The study proposes an allocation of responsibilities based on the Three Lines Model, ten quantitative indicators, a residual risk formula, and an integrated control maturity index with five levels. Scenario testing yielded a modelled aggregate-risk reduction from 135 to 47.84 points (64.56%); the scenario maturity index was 42.50%, versus a target of 80.00%. With nominal effectiveness fixed at 80%, lowering evidence reliability from 1.00 to 0.60 increases residual risk from 5.00 to 13.00. Scientific novelty lies in integrating regulatory, medical, information-security, and internal-audit requirements and using coefficient D to adjust control effectiveness and residual risk for evidence reliability. The practical value is that the matrix can serve as the basis for an internal control policy, an internal audit work programme, technical requirements for a medical information system, and a management dashboard. The scenario results demonstrate algorithmic consistency but do not constitute empirical evidence of effectiveness; the proposed parameters, weights, and thresholds require local calibration and validation on de-identified institutional data.
Keywords: *internal control; electronic medical documentation; electronic health system; medical information system; data quality; audit log; personal data protection; risk-based approach.*
Tabl.: *9.* ***Formulae:*** *6.* ***Bibl.:*** *19.*

Holovachko Vasyl M. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Accounting and Taxation and Marketing, Mukachevo State University (26 Uzhhorodska Str., Mukachevo, 89600, Ukraine)*
E-mail: *wasjahol1980@gmail.com*
ORCID: *https://orcid.org/0000-0002-5993-0873*

Herych Myroslava S. *– PhD (Physics and Mathematics), Associate Professor of the Department of Probability Theory and Mathematical Analysis, Uzhhorod National University (3 Narodna Sq., Uzhgorod, 88000, Ukraine)*
E-mail: *miroslava.gerich@uzhnu.edu.ua*
ORCID: *https://orcid.org/0000-0001-9634-5254*

Holovachko Anastasiia V. *– Master's Student, King Danylo Lviv National Medical University (69 Pekarska Str., Lviv, 79010, Ukraine)*
E-mail: *anastasiagolovacko@gmail.com*
ORCID: *https://orcid.org/0009-0006-9879-9229*

Цифровізація охорони здоров'я перетворила електронну медичну документацію з допоміжного інформаційного ресурсу на критичний елемент клінічних, управлінських і фінансових процесів закладу охорони здоров'я. Електронний запис одночасно підтверджує факт і зміст наданої допомоги, забезпечує безперервність лікування, формує інформаційну основу для оплати медичних послуг, аналізу результативності, планування ресурсів та оцінювання якості. Тому помилка, несвоєчасне внесення даних, невстановлене авторство або неправомірний доступ мають не лише інформаційні, а й клінічні, правові, репутаційні та економічні наслідки.

Масштаб об'єкта контролю стрімко зростає. За офіційними даними адміністратора електронної системи охорони здоров'я (ЕСОЗ), станом на квітень 2026 р. у центральній базі даних (ЦБД) ЕСОЗ накопичено майже 5,3 млрд електронних медичних записів щодо 34,6 млн пацієнтів, а щодня додається близько 2 млн нових записів [5]. За такого обсягу інформації суцільна ручна перевірка є неможливою, тоді як вибірковий контроль без автоматизованого аналізу журналів подій може не виявляти системних відхилень. Відповідно, внутрішній контроль має бути ризик-орієнтованим, безперервним і технологічно вбудованим у процес створення та використання документації.

Українська ЕСОЗ функціонує за двокомпонентною моделлю: медичні працівники взаємодіють із медичними інформаційними системами (МІС), а визначені дані передаються до ЦБД. Така архітектура розподіляє відповідальність між закладом, оператором МІС, адміністратором ЦБД та іншими суб'єктами, але не усуває відповідальності закладу за організацію власних процесів. Постанова Кабінету Міністрів України № 411 визначає засади функціонування ЕСОЗ [3], а наказ МОЗ України № 587 регулює ведення Реєстру медичних записів, записів про направлення та рецептів [4]. Водночас виконання формальних вимог до внесення даних не дорівнює наявності дієвої системи внутрішнього контролю.

Правова значущість електронної документації ґрунтується на можливості встановити її автора, перевірити цілісність, відтворити зміст і підтвердити послідовність оброблення. Закон України «Про електронні документи та електронний документообіг» поширює регулювання на створення, передавання, зберігання, використання та знищення електронних документів і вимагає зберігати їх у формі, що дає змогу перевірити цілісність [8]. Отже, контроль повинен охоплювати не тільки клінічний зміст запису, а й персональне підписання, часові мітки, версійність, права доступу та журнали подій.

Медичні дані належать до особливо чутливої інформації. Основи законодавства України про охорону здоров'я закріплюють вимоги щодо лікарської таємниці та прав пацієнта [7], а Закон України «Про захист персональних даних» установлює принципи законності, визначеної мети, пропорційності та за-

хищеності оброблення [9]. Європейський вектор розвитку посилює потребу в сумісності національних процедур із Регламентом (ЄС) 2025/327 про Європейський простір даних про здоров'я (*European Health Data Space – EHDS*), який установлює спільні правила первинного та вторинного використання електронних медичних даних і вимоги до систем електронних медичних записів (*electronic health record systems – EHR-систем*) [11].

Внутрішній контроль електронної медичної документації не можна зводити до кіберзахисту. Кібербезпека захищає систему від загроз, але не гарантує клінічної повноти, логічної узгодженості, своєчасності, достовірного авторства або належного виправлення помилок. Аналогічно медичний аудит може оцінювати якість допомоги, однак не завжди перевіряє конфігурацію ролей, актуальність облікових записів користувачів, повноту аудиторського сліду та відновлюваність даних. Потрібна інтегрована модель, яка поєднує управлінський, інформаційний, клінічний і технологічний контроль.

Проблема має виразний економічний вимір. Недостовірна документація спотворює показники діяльності, ускладнює підтвердження наданих послуг, підвищує витрати на повторне опрацювання записів, розслідування інцидентів і відновлення даних. Вона також знижує надійність інформації для калькулювання собівартості, бюджетування та оцінювання результативності підрозділів. Тому система контролю повинна створювати обґрунтовану впевненість у тому, що електронні медичні дані придатні не лише для лікування, а й для управлінських і фінансових рішень.

Актуальність дослідження зумовлена суперечністю між масштабом і складністю цифрових медичних процесів, з одного боку, та фрагментарністю організаційно-методичного забезпечення їх внутрішнього контролю – з іншого. У практиці закладів часто окремо регулюються інформаційна безпека, медична статистика, документування, захист персональних даних і внутрішній аудит. За відсутності єдиної карти ризиків та узгоджених показників виникають контрольні прогалини та дублювання процедур.

ОГЛЯД ЛІТЕРАТУРИ

Український науковий доробок підтверджує, що цифровізація медичних та обліково-управлінських процесів змінює не лише технічні засоби, а й відповідальність за якість даних. О. Білошицька, Л. Бондаренко та О. Бесараб пов'язують якість медико-статистичної інформації із застосуванням міжнародних стандартів медичної інформатики та семантичної сумісності [1]. В. Головачко, О. Королович і О. Гаврилець доводять, що автоматизація трансформує функціональний розподіл, аналітичні можливості та механізми прийняття рішень [2]. Отже, цифрову форму запису не можна вважати самостійним доказом його достовірності.

Дослідження взаємодії медичних працівників із МІС показують, що джерелом ризику є не тільки технічні збої, а й дизайн інтерфейсів, складність процесів, недостатнє навчання, дублювання дій і перевантаження користувачів. І. Сорока та співавтори узагальнили проблеми взаємодії операторів із медичними інформаційними системами та підкреслили значення ергономіки, стандартизації та навчальної підтримки [10]. Це вимагає включати до внутрішнього контролю аналіз причин помилок і коригування процесу, а не обмежуватися фіксацією порушень.

І. Максімова розглядає регулювання та організаційні форми внутрішнього аудиту закладів охорони здоров'я, підкреслюючи його незалежну оцінювальну та консультативну роль [6]. Водночас предметом дослідження є переважно загальна діяльність закладу та використання ресурсів. Методика контролю електронної медичної документації потребує конкретизації об'єктів, контрольних доказів, цифрових процедур і критеріїв оцінювання.

Міжнародні огляди систематизують виміри якості EHR-даних. Найчастіше оцінюються повнота, точність, узгодженість, правдоподібність і своєчасність, однак єдиного підходу до їх вимірювання немає [12; 16]. Тому загальні виміри якості необхідно перетворювати на локальні індикатори, правила перевірки та контрольні докази.

Дослідження аудит-логів виявляють неоднорідність визначень і процедур валідації [13; 18], а роботи з інтероперабельності акцентують на передаванні даних без втрати змісту [17]. ISO 27799:2025 та ISO/IEC 27001:2022 визначають вимоги до безпеки [14; 15], а Глобальні стандарти внутрішнього аудиту – до управління ризиками та доказовості [19]. Проте ці підходи не формують єдиної методики внутрішнього контролю електронної медичної документації.

Узагальнене порівняння наявних наукових підходів, їхніх обмежень і доповнень запропонованої авторської моделі наведено в *табл. 1.*

В опрацьованих джерелах [12–19] не виявлено єдиної ризик-орієнтованої моделі, яка поєднувала б життєвий цикл документації, ризики якості та конфіденційності, контрольні процедури, відповідальність, індикатори та надійність доказів.

МЕТА ТА ДОСЛІДНИЦЬКІ ПИТАННЯ

Метою статті є теоретичне обґрунтування та розроблення ризик-орієнтованої методики внутрішнього контролю електронної медичної до-

Таблиця 1

Порівняння наявних підходів із запропонованою ризик-орієнтованою моделлю

Наявний підхід	Обмеження для внутрішнього контролю електронної медичної документації	Доповнення авторської моделі
Оцінювання якості EHR-даних [12; 16]	Якість вимірюється відокремлено від доступу, авторства, контрольних процедур і залишкового ризику	Виміри якості перетворено на контрольні цілі, індикатори та процедури життєвого циклу документації
Аналіз EHR-аудит-логів [13; 18]	Наявність журналу не доводить виконання контролю; визначення та способи валідації різняться	Аудит-логи включено до доказів, а коефіцієнт D ураховує їх надійність
Семантична інтероперабельність та інформаційна безпека [14; 15; 17]	Фокус – безпечний обмін даними без інтегрованого контролю повноти, авторства, версійності та відповідальності	В одній матриці поєднано якість, доступ, цілісність, відновлюваність, інтероперабельність і треті сторони
Глобальні стандарти внутрішнього аудиту [19]	Загальні принципи не містять галузевих індикаторів і моделі залишкового ризику для медичної документації	Поєднано модель трьох ліній, десять індикаторів, індекс зрілості та залишковий ризик з урахуванням D

Джерело: систематизовано авторами на основі [12–19].

кументації, яка забезпечує узгоджене оцінювання законності, повноти, точності, своєчасності, конфіденційності, цілісності, доступності, простежуваності та інтероперабельності даних.

Для досягнення мети поставлено такі *завдання:* уточнити зміст об'єкта внутрішнього контролю; систематизувати нормативні та стандартні вимоги; ідентифікувати ризики на етапах життєвого циклу документації; визначити превентивні, виявляльні та коригувальні процедури; запропонувати систему показників і модель оцінювання зрілості контролю; виконати сценарне тестування й аналіз чутливості розробленого аналітичного інструментарію.

Дослідження відповідає на чотири питання: **RQ1** – які контрольні цілі повинні охоплювати електронну медичну документацію; **RQ2** – як поєднати контрольні процедури з ризиками її життєвого циклу; **RQ3** – за допомогою яких показників керівництво та внутрішній аудит можуть оцінювати результативність системи; **RQ4** – як надійність контрольного доказу впливає на скориговану результативність контролю та величину залишкового ризику.

МЕТОДИ ДОСЛІДЖЕННЯ

Методологічний дизайн ґрунтується на нормативно-документальному аналізі, структурованому цільовому огляді наукових публікацій, процесній декомпозиції, порівняльному зіставленні вимог і ризик-орієнтованому моделюванні. Предметом дослідження є організаційні та інформаційні процедури внутрішнього контролю, а об'єктом – життєвий цикл електронної медичної документації в закладі охорони здоров'я.

Під електронною медичною документацією в роботі розуміється сукупність електронних медичних записів, направлень, рецептів, висновків, протоколів, результатів досліджень, електронних форм первинної документації, пов'язаних метаданих, електронних підписів, версій і журналів подій, що створюються, передаються, зберігаються або використовуються закладом через МІС, ЕСОЗ і локальні інформаційні компоненти. Таке визначення є ширшим за окремий електронний медичний запис і дає змогу охопити доказовий контекст документа.

Інформаційну базу становили чинні українські нормативні акти щодо ЕСОЗ, медичних записів, охорони здоров'я, електронного документообігу та персональних даних [3; 4; 7–9], Регламент (ЄС) 2025/327 про Європейський простір даних про здоров'я [11], стандарти ISO 27799:2025 та ISO/IEC 27001:2022 [14; 15], Глобальні стандарти внутрішнього аудиту [19], офіційні статистичні дані ЕСОЗ [5] та рецензовані наукові праці 2020–2026 рр.

Структурований пошук проведено 12 серпня 2026 р. Пошук англомовних праць проведено в PubMed, а україномовних – в Open Ukrainian Citation Index (OUCI) та на сайтах відповідних журналів; додатково опрацьовано списки використаних джерел відібраних публікацій. Пошукові блоки: («electronic health record» OR EHR) AND («data quality» OR «audit log» OR interoperability OR privacy OR cybersecurity); («internal audit» AND healthcare AND («information system» OR «digital record»)); («електронна медична документація» OR

«медична інформаційна система») AND (якість OR контроль OR аудит OR стандартизація).

Критерії включення: 2020–2026 рр.; рецензований статус; зв'язок із предметом дослідження; перевірюваний DOI або сторінка журналу; доступна анотація чи повний текст українською або англійською. Виключено дублікати, препринти, нерецензовані й нерелевантні матеріали та праці без перевірюваних реквізитів. До аналітичного корпусу включено дев'ять статей [1; 2; 6; 10; 12; 13; 16–18]. Нормативні акти, стандарти й офіційну статистику аналізували окремо та до цієї кількості не включали.

На першому етапі з нормативних актів, стандартів і публікацій виокремлено вимоги до законності оброблення, якості, ідентифікації, підпису, доступу, зберігання, відновлення, простежуваності та передавання даних. На другому етапі життєвий цикл документації поділено на вісім контрольних ділянок: ідентифікація пацієнта; створення; перевірка та підписання; передавання; доступ і використання; виправлення та версійність; зберігання та відновлення; вторинне використання та експорт.

На третьому етапі для кожної ділянки сформовано зв'язок «ризик – контрольна ціль – процедура – доказ – індикатор». Процедури класифіковано як превентивні, виявляльні та коригувальні, а за способом виконання – як автоматизовані, автоматизовано-ручні та ручні. Такий поділ дає змогу відрізнити функціональність МІС від управлінського контролю, який передбачає призначену відповідальну особу, періодичність, критерій відхилення та документовану реакцію.

Для пріоритизації запропоновано оцінювати властивий ризик як добуток імовірності P та впливу I за п'ятибальною шкалою. Оцінка не претендує на універсальні нормативні пороги; заклад формує шкалу з урахуванням типу допомоги, критичності даних і власної історії інцидентів. Шкала є напівкількісною: бали відображають відносні рівні, а не статистичні ймовірності чи грошові оцінки, тому розрахунки використовуються для порівняльної пріоритизації, а не для прогнозування абсолютних втрат.

Для перевірки внутрішньої узгодженості методики проведено умовне сценарне тестування восьми ділянок життєвого циклу. Значення P та I охоплюють різні зони ризику, номінальна результативність контролю C варіює від 60% до 85%, а коефіцієнт надійності доказу D – від 0,75 до 0,95. Ці значення не є емпіричними даними конкретного закладу: вони використовуються для відтворюваної перевірки алгоритму, порівняння пріоритетів і однофакторного аналізу чутливості залишкового ризику до зміни D.

$$R_{inh} = P \cdot I, \text{ де } P, I \in \{1; 2; 3; 4; 5\}, \quad \textbf{(1)}$$

де R_{inh} – оцінка властивого ризику до застосування контрольних процедур, балів; P – імовірність реалізації ризикової події, балів; I – ступінь впливу ризикової події на клінічні, правові, операційні або економічні результати, балів.

P та I оцінюються за шкалою від 1 (мінімальне значення) до 5 (максимальне значення), тому R_{inh} може становити від 1 до 25 балів; вище значення означає вищий пріоритет ризику.

Для практичного застосування зміст рівнів 2–4 шкал P та I встановлюється локальним регламентом із зазначенням джерела оцінки, контрольного періоду та обґрунтування присвоєного бала. Якщо вплив оцінюється за кількома видами наслідків, правило їх агрегування – максимальне значення або документоване зважування – затверджується до початку тестування. У сценарному розрахунку значення P та I є модельними параметрами, а не емпіричними оцінками конкретного закладу.

Результативність контролю запропоновано оцінювати інтегральним індексом зрілості. Для кожного напряму встановлюється бал s від 0 до 4: 0 – контроль відсутній; 1 – фрагментарний; 2 – формалізований; 3 – інтегрований і систематично виконується; 4 – адаптивний (автоматизований, аналітично керований і такий, що безперервно вдосконалюється). Ваги w затверджує керівництво, їх сума дорівнює одиниці.

$$IC_{EMD} = \left(\frac{\sum_{j=1}^{m} w_j s_j}{4} \right) \cdot 100\%, \; , \sum_{j=1}^{m} w_j = 1, \quad \textbf{(2)}$$

де IC_{EMD} – інтегральний індекс зрілості внутрішнього контролю електронної медичної документації, %; w_j – вага j-го напряму контролю ($0 \le w_j \le 1$); s_j – оцінка зрілості j-го напряму за шкалою від 0 до 4; j – порядковий номер напряму; m – кількість напрямів (у сценарному розрахунку $m = 6$), а підсумовування здійснюється за $j = 1, \ldots, m$; 4 – максимальна оцінка зрілості.

Значення IC_{EMD} належить інтервалу 0–100%, а його зростання свідчить про підвищення формалізації, інтегрованості й автоматизації контролю.

Щоб не прирівнювати наявність процедури до доведеної результативності, введено коефіцієнт надійності доказу D. Він охоплює: d_1 – прямоту й автентичність (первинна система, автор, джерело, час і цілісність); d_2 – повноту реквізитів, подій, періоду та сукупності; d_3 – своєчасність і відповідність контрольному періоду; d_4 – відтворюваність результату незалежним фахівцем. Кожний компонент d_k набуває значення від 0 до 1 і визначається за п'ятьма ознаками, наведеними далі.

Підсумкове значення:

$$D = \sum_{k=1}^{4} \alpha_k d_k, \ \sum_{k=1}^{4} \alpha_k = 1, \ 0 \le d_k \le 1. \quad (3)$$

У сценарії застосовано рівні ваги $\alpha_k = 0{,}25$, тому $D = 0{,}25 \cdot (d_1 + d_2 + d_3 + d_4)$. Значення $0{,}80 \le D \le 1{,}00$ – висока надійність; $0{,}60 \le D \le 0{,}80$ – середня надійність; $0 \le D \le 0{,}60$ – низька надійність.

Для операціоналізації коефіцієнта D кожний його компонент оцінюється за п'ятьма ознаками. Для d_1 такими ознаками є походження доказу з первинної системи, ідентифікованість автора або джерела, наявність довіреної часової позначки, підтвердження цілісності та простежуваність походження; для d_2 – охоплення обов'язкових реквізитів, подій, контрольного періоду, досліджуваної сукупності та виявлених винятків; для d_3 – формування доказу в установлений строк, відповідність контрольному періоду, доступність на дату перевірки, належна періодичність оновлення та врахування запізнілих подій; для d_4 – документованість методики, доступність вихідних даних, збереження параметрів перевірки, можливість незалежного повторного виконання та наявність аудиторського сліду результату.

Кожна ознака отримує 0 балів, якщо її не підтверджено; 0,5 бала – якщо підтверджено частково; 1 бал – якщо підтверджено повністю. Значення відповідного компонента d_k визначається як середнє арифметичне п'яти оцінок, що забезпечує крок шкали 0,10. Наведені в *табл. 2* значення є модельними параметрами авторського сценарію, а не результатами аудиту конкретного закладу.

Компонентна декомпозиція показує, що найвища сценарна надійність доказів характерна для перевірки та підписання, а також для зберігання та відновлення, де використовуються журнали електронних підписів, історія версій, протоколи відновлення та результати повторного тестування. Нижче значення D для вторинного використання зумовлене сценарними обмеженнями повноти доказів щодо мети оброблення, складу переданих даних і можливості незалежного відтворення результатів. Така декомпозиція забезпечує простежуваність установлених значень D та дає змогу під час практичного застосування моделі замінити сценарні оцінки фактичними результатами контрольного тестування.

Скоригована результативність C_{eff} дорівнює $C \cdot D$.

$$C_{eff} = C \cdot D, \quad (4)$$

де C_{eff} – скоригована результативність контролю, %; C – номінальна результативність контролю, %; D – коефіцієнт надійності контрольного доказу, що набуває значень від 0 до 1.

Номінальна результативність контролю C у практичному застосуванні визначається за затвердженою програмою тестування як зважена частка успішно виконаних контрольних тестів. Для кожного тесту документуються критерій, період, досліджувана сукупність або вибірка, результат і критичність виявленого винятку. У сценарному розрахунку значення C є модельними припущеннями та не характеризують фактичну результативність контролю конкретного закладу.

За $D = 1$ номінальна результативність підтверджена повністю; за $D < 1$ вона пропорційно зменшується, тому C_{eff} не може перевищувати C.

Залишковий ризик визначається з урахуванням скоригованої результативності контрольних заходів. Формула використовується як управлінський інструмент пріоритизації та не підмінює професійного судження внутрішнього аудитора.

$$R_{res} = R_{inh} \cdot (1 - C_{eff} / 100), \quad (5)$$

Таблиця 2

Компонентна декомпозиція коефіцієнта надійності контрольного доказу у сценарному розрахунку

Етап життєвого циклу	d_1: прямота й автентичність	d_2: повнота	d_3: своєчасність	d_4: відтворюваність	D
Ідентифікація	1,00	0,90	0,90	0,80	0,90
Створення	0,90	0,80	0,90	0,80	0,85
Перевірка і підпис	1,00	0,90	1,00	0,90	0,95
Передавання	1,00	0,90	0,80	0,90	0,90
Доступ і використання	0,90	0,80	0,80	0,70	0,80
Виправлення та версії	0,90	0,90	0,80	0,80	0,85
Зберігання та відновлення	1,00	1,00	0,90	0,90	0,95
Вторинне використання	0,80	0,70	0,80	0,70	0,75

Джерело: авторська сценарна декомпозиція; значення модельні та не характеризують конкретний медичний заклад.

де R_{res} – оцінка залишкового ризику після врахування контролю, балів; R_{inh} – оцінка властивого ризику, балів; C_{eff} – скоригована результативність контролю, %.

Ділення C_{eff} на 100 переводить відсоткове значення в частку: за C_{eff} = 0% залишковий ризик дорівнює властивому, а за C_{eff} = 100% у межах розрахункової моделі дорівнює нулю. Менше значення R_{res} означає нижчий пріоритет неврегульованого ризику.

Дослідження не передбачало залучення пацієнтів, медичних працівників як респондентів або оброблення персональних медичних даних, тому схвалення комісією з етики не вимагалося. Запропоновані пороги та процедури повинні пройти локальну апробацію до використання для оцінювання конкретного закладу.

РЕЗУЛЬТАТИ

Контрольні цілі та межі відповідальності

Внутрішній контроль електронної медичної документації пропонується визначати як організовану керівництвом сукупність політик, розподілу відповідальності, автоматизованих правил, перевірок і коригувальних дій, що надає обґрунтовану, але не абсолютну впевненість у законності, якості, захищеності, доступності та простежуваності документації протягом її життєвого циклу. Визначення акцентує на управлінській відповідальності: технічна наявність журналу або електронного підпису ще не означає, що їх регулярно перевіряють і використовують для реагування.

Контрольний об'єкт має три взаємопов'язані рівні. Перший – *змістовий:* клінічні відомості, реквізити, коди, дати, результати та взаємозв'язки між записами. Другий – *доказовий:* ідентифікатор автора, підпис, час, версія, підстава виправлення, джерело та маршрут передачі. Третій – *системний:* ролі доступу, конфігурація МІС, інтеграційні інтерфейси, резервні копії, журнали подій і договори з постачальниками.

На основі аналізу сформовано дев'ять контрольних цілей: 1) законність і визначена мета оброблення; 2) правильна ідентифікація пацієнта; 3) повнота; 4) точність і правдоподібність; 5) своєчасність; 6) конфіденційність і мінімально необхідний доступ; 7) цілісність та авторство; 8) доступність і відновлюваність; 9) простежуваність та інтероперабельність. Їх взаємозв'язок із джерелами вимог наведено в *табл. 3*.

Зазначені цілі слід застосовувати диференційовано. Наприклад, для алергічного статусу, групи крові або критичного лабораторного результату пріоритетними є точність, своєчасність і доступність; для психіатричних, ВІЛ-пов'язаних або інших чутливих даних додатково підвищуються вимоги до конфіденційності; для інформації, що під-

Таблиця 3

Система контрольних цілей електронної медичної документації

№ з/п	Контрольна ціль	Зміст критерію	Джерело
1	Законність і визначена мета	Наявність правової підстави, обмеження мети, мінімізація даних, дотримання прав пацієнта	[7; 9; 11]
2	Правильна ідентифікація	Однозначне зіставлення запису з пацієнтом; попередження дублетів та помилкового вибору картки	[3; 4]
3	Повнота	Заповнення обов'язкових реквізитів і наявність даних, необхідних для клінічного та управлінського використання	[12; 16]
4	Точність і правдоподібність	Відповідність фактичній події, допустимим значенням, одиницям виміру та логічним зв'язкам	[1; 12; 16]
5	Своєчасність	Створення, підписання, передавання й виправлення запису у визначені строки	[4; 12]
6	Конфіденційність і доступ	Ідентифікація користувача, найменші необхідні повноваження, контроль чутливих даних і невідкладного доступу	[9; 14; 15]
7	Цілісність та авторство	Неможливість непомітної зміни; підтвердження автора, часу та справжності документа	[8; 14]
8	Доступність і відновлюваність	Доступ уповноваженим користувачам, резервування, відновлення і безперервність критичних процесів	[8; 14; 15]
9	Простежуваність та інтероперабельність	Повний аудиторський слід і передавання даних без втрати змісту	[1; 13; 17; 18]

Джерело: розроблено авторами на основі [1; 3; 4; 7–9; 11–18].

тверджує надану послугу, важливими є авторство, повнота та простежуваність. Універсальний перелік цілей не означає однакової ваги для всіх типів записів.

Система повинна охоплювати як дані, передані до ЦБД ЕСОЗ, так і локальні документи закладу. Контроль лише статусу успішної передачі створює хибну впевненість: повідомлення може бути технічно прийняте, але містити помилковий код, неповний зміст або посилання на неправильного пацієнта. Тому технічну квитанцію необхідно доповнювати логічною та змістовою валідацією.

Ризик-орієнтована модель за життєвим циклом

Життєвий цикл документації починається до моменту введення клінічного тексту – з ідентифікації пацієнта, користувача та контексту події. Помилка на цьому етапі поширюється на подальші записи, направлення, рецепти, рахунки та аналітичні звіти. Превентивний контроль має включати пошук потенційних дублетів, перевірку ключових ідентифікаторів і обмеження ручного створення нового профілю без повторного пошуку.

На етапі створення основними ризиками є пропуски обов'язкових даних, використання невідповідних шаблонів, копіювання застарілої інформації, суперечності між полями та надмірний вільний текст. Автоматизовані правила повинні блокувати критичні пропуски, а м'які попередження – звертати увагу на нетипові або суперечливі значення. Водночас надмірна кількість попереджень спричиняє втому від сповіщень, тому їх ефективність необхідно аналізувати за частотою ігнорування та клінічною значущістю.

Підписання та блокування завершеного запису відокремлюють робочий чернетковий стан від юридично значущої документації. Контроль повинен підтвердити, що підпис належить уповноваженій особі, застосований до правильної версії, а подальше виправлення здійснюється через нову версію або доповнення із зазначенням автора, часу та причини. Перезапис первинного значення без збереження історії є неприйнятною контрольною прогалиною.

На етапі доступу важливо відрізняти автентифікацію від авторизації. Навіть належно ідентифікований користувач може мати надлишкові права. Тому ролі слід формувати за функціями, підрозділом, контекстом лікування та чутливістю даних, а не лише за посадою. Особливий режим невідкладного доступу має реєструвати підставу та підлягати подальшому обов'язковому перегляду.

Журнали подій є центральним доказом простежуваності, але їх накопичення без сценаріїв аналізу не створює контролю. Доцільно визначити ознаки аномалій: масовий перегляд карток, доступ поза робочим часом без службової потреби, звернення до даних осіб, не пов'язаних із лікуванням, повторні невдалі входи, експорт значного масиву, нетипову частоту виправлень або використання невідкладного доступу. Результат автоматичного відбору повинен мати власника, строк розгляду та документований висновок.

Резервне копіювання є лише превентивною передумовою відновлення. Контрольним доказом слід вважати успішний тест відновлення з перевіркою цілісності, повноти та прийнятного часу відновлення. Аналогічно договір з оператором МІС не замінює контролю третьої сторони: заклад має визначити вимоги до повідомлення про інциденти, журналювання, експорту даних, припинення договору та повернення або знищення копій.

У *табл. 4* наведено узагальнену матрицю, яку заклад може деталізувати за типами допомоги та функціональними модулями. Вона не встановлює універсальної періодичності: висока критичність передбачає безперервний автоматизований моніторинг, тоді як низькоризикові процедури можуть перевірятися вибірково.

Організаційна модель і розподіл відповідальності

Ефективність методики залежить від розмежування володіння процесом і незалежного оцінювання. Клінічні підрозділи відповідають за правильність і своєчасність документування; служба інформаційних технологій – за доступність, конфігурацію та технічні журнали; відповідальна особа із захисту даних – за законність і права суб'єктів; служба якості – за клінічні критерії; внутрішній аудит – за незалежну оцінку дизайну та виконання контролів. Передання ІТ-функцій оператору МІС не означає передання йому управлінської відповідальності закладу.

Доцільною є модифікована модель трьох ліній. Перша лінія виконує операційні контроли під час створення та використання документації. Друга встановлює правила, моніторить відповідність, аналізує інциденти та консультує. Третя незалежно перевіряє, чи правильно визначено ризики, чи працюють ключові контроли й чи достовірними є управлінські звіти. Нагляд здійснює керівник або колегіальний орган, який затверджує прийнятний ризик і план поліпшення.

Особливу увагу слід приділяти конфлікту функцій. Адміністратор, який надає права, не повинен одноосібно підтверджувати їх належність; працівник, який вносить виправлення, не повинен бути

Таблиця 4

Матриця ризиків і процедур внутрішнього контролю електронної медичної документації

Етап	Ключові ризики	Основні контрольні процедури	Контрольні докази
Ідентифікація	Помилковий пацієнт; дублет профілю; неправильний контекст звернення	Пошук збігів; перевірка ключових ідентифікаторів; обмеження створення дублетів	Звіт потенційних дублетів; протокол об'єднання
Створення	Пропуски; суперечності; копіювання застарілих даних; неправильний шаблон	Обов'язкові поля; довідники; логічні та діапазонні перевірки; контроль copy-forward	Звіт помилок валідації; вибіркова змістова перевірка
Перевірка та підпис	Непідписаний запис; підпис іншої особи; запізніле завершення	Персональна автентифікація; контроль статусу; часові обмеження; перевірка сертифіката	Реєстр непідписаних і прострочених записів; журнал підписів
Передавання	Втрата повідомлення; дублювання; помилка кодування; семантична невідповідність	Контроль квитанцій; звірка кількості; тестування зіставлення даних; повторне передавання із забезпеченням ідемпотентності	Звіт відхилених/повторних повідомлень; протокол інтеграційної звірки
Доступ і використання	Надлишкові права; неактуальний обліковий запис; нецільовий перегляд; зловживання невідкладним доступом	RBAC/ABAC; MFA; життєвий цикл облікового запису; періодичне підтвердження прав; постконтроль невідкладного доступу	Матриця ролей; реєстр погоджень; звіт аномальних доступів
Виправлення та версії	Непомітна зміна; відсутня причина; суперечливі версії	Заборона перезапису; доповнення/нова версія; обов'язкова причина; зв'язок із первинним записом	Історія версій; журнал виправлень; акт перевірки
Зберігання та відновлення	Втрата; пошкодження; недоступність; невідновлювана резервна копія	Резервування; контроль цілісності; тест відновлення; план безперервності; моніторинг доступності	Протокол відновлення; звіт RTO/RPO; журнал інцидентів
Вторинне використання	Надмірний експорт; повторна ідентифікація; використання поза метою	Погодження мети; мінімізація; псевдонімізація; контроль набору й одержувача; строк зберігання	Реєстр наборів і передач; рішення уповноваженої особи; журнал експорту

Примітка: copy-forward – перенесення даних із попереднього запису; emergency access – невідкладний доступ; RBAC – рольове керування доступом; ABAC – атрибутне керування доступом; MFA – багатофакторна автентифікація; RTO – цільовий час відновлення; RPO – цільова точка відновлення.

Джерело: розроблено авторами на основі [3; 4; 8; 9; 11–19].

єдиним оцінювачем обґрунтованості; розробник автоматизованого правила не повинен самостійно приймати його в експлуатацію без тестування власником процесу. Для невеликих закладів, де повне розмежування неможливе, застосовуються компенсувальні контроли – регулярний перегляд керівником, вибіркова незалежна звірка та зовнішня оцінка.

Узагальнений розподіл повноважень і відповідальності між учасниками системи внутрішнього контролю наведено в *табл. 5*.

Організаційним ядром системи є реєстр ключових контролів. Для кожного контролю доцільно зазначати ризик, ціль, власника, опис процедури, частоту, джерело даних, доказ виконання, критерій винятку, строк реагування та компенсувальний контроль. Такий реєстр усуває ситуацію, коли процедура формально передбачена положенням, але її виконання неможливо підтвердити.

Показники результативності та програма перевірки

Для переходу від декларативного до вимірюваного контролю запропоновано систему індикаторів, наведену в *табл. 6*. Вона поєднує якість документації, управління доступом, простежуваність, інтероперабельність і безперервність. Показники не повинні використовуватися ізольовано: високий відсоток технічно заповнених полів може поєднуватися з низькою клінічною правильністю, а відсутність зареєстрованих інцидентів може свідчити не про безпеку, а про слабке виявлення.

Таблиця 5

Розподіл відповідальності за внутрішній контроль

Рівень	Основні учасники	Відповідальність
Перша лінія	Лікарі, медичні сестри, реєстратура, лабораторії, локальні адміністратори процесів	Коректне документування; первинна перевірка; повідомлення про помилки та інциденти
Друга лінія	Служба якості, захист даних, комплаєнс, інформаційна безпека, медична статистика	Політики та критерії; моніторинг показників; аналіз винятків; методична підтримка
Третя лінія	Внутрішній аудит або незалежна контрольна функція	Оцінка дизайну, виконання та доказовості контролів; рекомендації; контроль виконання заходів
Нагляд	Керівник закладу, медична рада, комітет з якості/аудиту	Затвердження ризик-апетиту, відповідальності, ресурсів, планів усунення та звітності

Джерело: розроблено авторами з урахуванням [6; 19].

Для полів із формалізованими правилами доцільний автоматизований суцільний аналіз 100% записів. Він охоплює пропуски, дублети, допустимі діапазони, часову послідовність, статус підпису, відхилені повідомлення, неактуальні облікові записи та аномальні події доступу. Ручна перевірка використовується для клінічного змісту, обґрунтованості виправлень і відповідності доступу фактичним обов'язкам.

Вибірку для ручної перевірки слід формувати стратифіковано за типом документа, підрозділом, зміною, автором, рівнем чутливості та результатами автоматичних правил. До випадкової частини додаються цільові записи з підвищеним ризиком. Це знижує ймовірність того, що перевірка охопить лише типові записи та не виявить рідкісні, але критичні порушення.

Універсальні цільові значення для всіх закладів не пропонуються, оскільки критичність даних і процеси відрізняються. Керівництво затверджує пороги, виходячи з правових вимог, клінічного ризику, технічних можливостей і базового рівня. Для критичних ідентифікаційних реквізитів та авторства прийнятність відхилень має бути значно нижчою, ніж для другорядних описових полів.

Для управлінської звітності показники доцільно подавати не лише поточним значенням, а й трендом, розподілом за підрозділами, критичністю винятків та статусом заходів. Агрегований «зелений» статус не повинен приховувати одиничне критичне порушення, наприклад неправомірний доступ до чутливих даних або неможливість відновити архів. Тому інтегральний індекс доповнюється переліком критичних винятків, які не компенсуються середнім балом.

Програма внутрішньої перевірки повинна містити п'ять блоків: оцінювання дизайну; тест виконання; повторне виконання автоматизованого правила на контрольному наборі; аналіз журналів і винятків; перевірку коригувальних дій. Доказами можуть бути конфігурації ролей, витяги з журналів, протоколи відновлення, звіти валідації, квитанції обміну, історія версій, погодження доступу та результати повторного тесту. Скріншот без збережених параметрів і джерела даних має обмежену доказову силу.

Оцінювання зрілості та послідовність упровадження

Інтегральний індекс IC_{EMD} доцільно розраховувати за шістьма напрямами: управління та відповідальність – 15%; якість документації – 20%; доступ і конфіденційність – 20%; цілісність та простежуваність – 20%; безперервність – 15%; інтероперабельність і треті сторони – 10%. Ваги є рекомендованими та можуть змінюватися за умови документованого обґрунтування. Установлення підвищеної ваги конфіденційності не повинно зменшувати значущість клінічної точності до неприйнятного рівня. Зміст рівнів зрілості внутрішнього контролю та критерії їх ідентифікації наведено в *табл. 7*.

Сценарне тестування та аналіз чутливості

Для аналітичної перевірки запропонованої методики сформовано умовний сценарій, у якому кожній із восьми ділянок життєвого циклу присвоєно оцінки *P, I, C* і *D*. Розрахунки в *табл. 8* є ілюстративними, а не результатом спостереження за конкретним закладом. Їх мета – перевірити логічну узгодженість формул, продемонструвати вплив доказовості контролю та визначити, чи зберігає модель управлінську пріоритетність ризиків.

Таблиця 6

Ключові індикатори внутрішнього контролю

Індикатор	Формула	Контрольне призначення
Повнота критичних реквізитів	$K_1 = \frac{n\text{ (обов'язкових значень)} - n\text{ (пропусків)}}{n\text{ (обов'язкових значень)}}$	Якість документації; за типом поля та підрозділом
Своєчасність завершення	$K_2 = \frac{n\text{ (завершено у строк)}}{n\text{ (записів,що підлягали завершенню)}}$	Дотримання строків; аналіз причин прострочення
Частка потенційних дублетів	$K_3 = \frac{n\text{ (потенційних дублетів)}}{n\text{ (активних профілів)}}$	Якість ідентифікації пацієнтів
Простежуваність виправлень	$K_4 = \frac{n\text{ (простежуваних виправлень)}}{n\text{ (усіх виправлень)}}$	Цілісність і версійність
Покриття перегляду прав	$K_5 = \frac{n\text{ (облікових записів із підтвердженими правами)}}{n\text{ (активних облікових записів)}}$	Управління доступом
Закриття аномалій у строк	$K_6 = \frac{n\text{ (аномалій, розглянутих у строк)}}{n\text{ (аномалій, що підлягали розгляду)}}$	Дієвість моніторингу журналів
Успішність інтеграційного звіряння	$K_7 = \frac{n\text{ (підтверджених коректних передач)}}{n\text{ (ініційованих передач)}}$	Технічна та семантична інтероперабельність
Успішність тестів відновлення	$K_8 = \frac{n\text{ (успішних тестів)}}{n\text{ (запланованих тестів)}}$	Відновлюваність і безперервність
Середній час усунення	$K_9 = \frac{1}{N}\sum_{i=1}^{n}\left(t_i^{\text{усунення}} - t_i^{\text{виявлення}}\right)$, де N – кількість закритих відхилень	Швидкість коригувальної реакції
Повторюваність відхилень	$K_{10} = \frac{n\text{ (повторних відхилень)}}{n\text{ (усунених відхилень)}}$	Стійкість коригувальних дій

Примітка: $n(\cdot)$ – кількість відповідних об'єктів або подій; простежуваним є виправлення, для якого зафіксовано автора, час і причину. Зростання K_1, K_2, K_4–K_8 свідчить про поліпшення контролю; для K_3, K_9 і K_{10} нижче значення є кращим. За нульового знаменника показник позначають «н/з», а не прирівнюють до нуля.

Джерело: розроблено авторами з урахуванням вимірів якості [12; 16] та підходів до журналів подій [13; 18].

$$\Delta R = \left(\frac{\sum R_{inh} - \sum R_{res}}{\sum R_{inh}}\right)\cdot 100\%, \qquad \textbf{(6)}$$

де ΔR – відносне скорочення сукупного ризику після застосування контролів, %; ΣR_{inh} – сума оцінок властивого ризику за всіма ділянками, балів; ΣR_{res} – сума оцінок залишкового ризику за цими ділянками, балів.

Додатне значення ΔR характеризує частку зниження портфельного ризику; показник потрібно інтерпретувати разом з абсолютними значеннями R_{res}, щоб інтегральне поліпшення не приховувало критичних ділянок. Агрегування є коректним для ділянок, оцінених за однаковою шкалою; за різної критичності мають застосовуватися документовані ваги.

За сценарієм сукупний властивий ризик становить ΣR_{inh} = 135 балів, а сукупний залишковий ризик – ΣR_{res} = 47,84 бала. Відносне скорочення портфельного ризику дорівнює ΔR = ((135 – 47,84) / 135) × 100% = 64,56%. Після врахування контролів найвищий пріоритет зберігають вторинне використання даних (R_{res} = 11,00) та доступ і використання (R_{res} = 9,00), тоді як для перевірки та підписання R_{res} = 2,89. Отже, модель не маскує високий властивий ризик номінальною наявністю процедури, а спрямовує ресурси на ділянки з найбільшим неврегульованим впливом.

Таблиця 7

Рівні зрілості внутрішнього контролю електронної медичної документації

Рівень	Характеристика
0 – відсутній	Процедури не визначені; контрольні докази не формуються; реагування лише після значного інциденту
1 – фрагментарний	Окремі ручні перевірки залежать від ініціативи працівників; відповідальність і критерії непослідовні
2 – формалізований	Затверджено політики, ролі, періодичність і форми доказів; автоматизація обмежена
3 – інтегрований	Контроли вбудовані у процеси та МІС; показники регулярно аналізуються; винятки мають власників і строки
4 – адаптивний	Автоматизований та аналітично керований контроль; суцільна аналітика формалізованих даних, ризик-орієнтовані сценарії, перевірена відновлюваність і безперервне вдосконалення

Джерело: розроблено авторами.

Таблиця 8

Сценарний розрахунок залишкового ризику за етапами життєвого циклу

Етап	P	I	R_{inh}	C, %	D	C_{eff}, %	R_{res}
Ідентифікація	4	5	20	80	0,90	72,00	5,60
Створення	4	4	16	70	0,85	59,50	6,48
Перевірка і підпис	3	5	15	85	0,95	80,75	2,89
Передавання	3	4	12	75	0,90	67,50	3,90
Доступ і використання	5	5	25	80	0,80	64,00	9,00
Виправлення та версії	3	4	12	65	0,85	55,25	5,37
Зберігання та відновлення	3	5	15	80	0,95	76,00	3,60
Вторинне використання	4	5	20	60	0,75	45,00	11,00
Разом / портфель	–	–	135	–	–	–	47,84

Джерело: авторські розрахунки; значення є сценарними та не характеризують конкретний заклад.

Аналіз чутливості підтверджує суттєвість коефіцієнта *D*. За незмінних R_{inh} = 25 і *C* = 80% повний доказ (*D* = 1,00) формує R_{res} = 25 × (1 – 0,80) = 5,00; за *D* = 0,80 залишковий ризик зростає до 9,00; за *D* = 0,60 – до 13,00. Ігнорування ненадійності доказу в останньому випадку дає оцінку 5,00 замість 13,00, тобто занижує її на 8 балів (61,54% від скоригованого значення); скоригований ризик є у 2,60 разу вищим за номінальну оцінку. Таким чином, окрема перевірка доказовості є не формальною деталлю, а параметром, що істотно змінює управлінське рішення.

Для визначення розриву між базовим і цільовим профілями зрілості виконано сценарний розрахунок, результати якого наведено в *табл. 9*.

Розрахунок за формулою (2) дає базове сценарне значення IC_{EMD} = 42,50%, що відповідає формалізованому, але недостатньо інтегрованому контролю. Цільовий сценарний профіль формує IC_{EMD} = 80,00%; розрив між базовим і цільовим сценарними значеннями становить 37,50 відсоткового пункту, або 88,24% від базового рівня. Декомпозиція показує, що найбільший внесок у розрив створюють доступ і конфіденційність (+10,00 в. п.) та цілісність і простежуваність (+10,00 в. п.). Саме ці напрями доцільно включити до першої хвилі вдосконалення, а інтегральний індекс використовувати разом із абсолютними значеннями критичних ризиків.

Упровадження методики доцільно здійснювати поетапно: інвентаризувати інформаційні потоки та типи документації; визначити власників процесів, критичні дані та чинні контроли; сформувати карту ризиків і виявити прогалини; апробувати автоматичні правила, ручну вибірку, звіт винятків і цикл коригування на одному структурованому процесі, наприклад електронних направленнях, лабораторних результатах або завершенні амбулаторних взаємодій; після оцінки хибнопозитивних спрацювань масштабу-

Таблиця 9

Сценарна оцінка базового та цільового індексу зрілості

Напрям	w_j	Базовий рівень: s_0 / внесок, %	Цільовий рівень: s_1 / внесок, %
Управління та відповідальність	0,15	2 / 7,50	3 / 11,25
Якість даних	0,20	2 / 10,00	3 / 15,00
Доступ і конфіденційність	0,20	1 / 5,00	3 / 15,00
Цілісність і простежуваність	0,20	2 / 10,00	4 / 20,00
Безперервність	0,15	2 / 7,50	3 / 11,25
Інтероперабельність і треті сторони	0,10	1 / 2,50	3 / 7,50
Разом / інтегральне значення	1,00	1,70 / 42,50	3,20 / 80,00

Примітка: ваги та бали мають бути локально валідовані.

Джерело: авторські розрахунки.

вати правила. Для мінімізації документального навантаження слід повторно використовувати дані MIC і журналів подій, застосовуючи ручне підтвердження лише за недостатності автоматизованого доказу. Результативність оцінюють за динамікою повторних відхилень, часом реагування та надійністю документації; постійне накопичення структурованих доказів водночас підвищує готовність до зовнішніх перевірок і простежуваність впливу управлінських рішень на ризик.

ОБГОВОРЕННЯ

Отримані результати підтверджують, що внутрішній контроль електронної медичної документації слід розглядати ширше за перевірку заповнення форм. Наукові огляди якості EHR-даних виділяють повноту, правильність, узгодженість, правдоподібність і актуальність [12; 16], тоді як запропонована модель доповнює їх законністю, авторством, доступністю, простежуваністю та інтероперабельністю. Це розширення зумовлене подвійною природою медичного документа: він є джерелом клінічної інформації та юридично значущим цифровим доказом.

Висновок про необхідність аналізувати журнали подій узгоджується з A. Rule et al. [18] та Y. Huilgol et al. [13]. Водночас у цьому дослідженні аудит-логи включено не як окремий масив для дослідження поведінки, а як доказовий шар кожної контрольної цілі. Такий підхід дає змогу пов'язувати подію доступу з роллю, пацієнтом, документом, метою та подальшою реакцією, а також оцінювати не лише наявність, а й відтворюваність контрольного доказу.

Порівняння з ISO 27799:2025 і ISO/IEC 27001:2022 показує відповідність запропонованої методики ризик-орієнтованій логіці та принципам конфіденційності, цілісності й доступності [14; 15]. Водночас стаття конкретизує загальні стандарти до життєвого циклу медичної документації та доповнює їх показниками повноти, своєчасності, виправлень та інтеграційної звірки.

Семантична сумісність, яку досліджують S. Palojoki et al. [17] та українські автори [1], у методиці виділена окремою контрольною ціллю. Це має практичне значення для двокомпонентної архітектури ЕСОЗ: успішне технічне передавання не гарантує збереження медичного змісту. Контроль зіставлення довідників, одиниць і статусів повинен бути частиною приймання нової версії інтеграції.

Сценарне тестування та однофакторний аналіз чутливості підтвердили внутрішню узгодженість моделі та показали, що коригування на *D* змінює пріоритетність ризиків. Агреговані показники слід використовувати разом із профілем за напрямами та реєстром критичних винятків, щоб загальне поліпшення не приховувало окремих критичних ділянок.

Наукова новизна дослідження полягає в розробленні інтегрованої ризик-орієнтованої методики, що поєднує дев'ять контрольних цілей, вісім ділянок життєвого циклу, три типи процедур, систему доказів, десять індикаторів та п'ятирівневу шкалу зрілості. Додатковим внеском є коефіцієнт надійності доказу *D*, який перетворює номінальну результативність на скориговану та безпосередньо впливає на залишковий ризик. На відміну від підходів, орієнтованих лише на кіберзахист або клінічну якість, модель охоплює управлінсько-економічні наслідки достовірності документації.

Практична цінність полягає в можливості використати матрицю як основу положення про внутрішній контроль, робочої програми аудиту, технічного завдання до MIC та управлінської панелі показників. Методика масштабується від ручної

вибірки критичних контролів у невеликому закладі до суцільної автоматизованої аналітики в багатопрофільній лікарні. Витрати на її впровадження доцільно розглядати як інвестицію у зменшення ризику втрат, повторної роботи, претензій і викривлених управлінських рішень.

Обмеження дослідження пов'язані з *відсутністю доступу до знеособлених записів та аудит-логів конкретного закладу*. Сценарні розрахунки демонструють внутрішню узгодженість і чутливість інструментарію, але не доводять фактичного ефекту контролів. Через це не оцінювалися емпірична частота ризиків, кореляція індексу зрілості з клінічними результатами або фінансовими втратами; параметри, ваги та пороги потребують локальної калібрації та зовнішньої валідації.

Друге обмеження полягає у *відмінностях між MIC, профілями закладів і моделями організації допомоги*. Окремі автоматизовані правила можуть бути технічно недоступними без доопрацювання постачальника. Крім того, нормативне середовище ECO3 і EHDS продовжує розвиватися, тому реєстр контролів повинен містити процедуру регулярного оновлення.

Перспективою подальших досліджень є апробація моделі на знеособлених даних кількох закладів, визначення базових розподілів показників, оцінювання хибнопозитивних сценаріїв доступу та зв'язку між якістю документації, відхиленнями в оплаті, повторним опрацюванням і клінічними інцидентами. Окремого дослідження потребує застосування машинного навчання для виявлення аномалій за умови пояснюваності та контролю упереджень.

ВИСНОВКИ

Електронна медична документація є критичним інформаційним активом, від якого залежать безперервність допомоги, захист прав пацієнта, підтвердження діяльності, фінансування та управлінська аналітика. Тому її внутрішній контроль повинен охоплювати не лише інформаційну безпеку, а весь життєвий цикл і зміст даних.

За результатами дослідження визначено дев'ять контрольних цілей: законність і визначена мета; правильна ідентифікація; повнота; точність і правдоподібність; своєчасність; конфіденційність і мінімально необхідний доступ; цілісність та авторство; доступність і відновлюваність; простежуваність та інтероперабельність. Їх реалізація потребує узгодження автоматизованих правил MIC, ручних професійних перевірок і незалежної оцінки.

Запропонована матриця пов'язує вісім етапів життєвого циклу з ризиками, процедурами та доказами. Центральними елементами є запобігання дублетам, логічна валідація, персональне підписання, контроль передачі, найменші необхідні права, незмінна історія версій, перевірене відновлення та контроль вторинного використання.

Розроблено десять індикаторів і п'ятирівневу модель зрілості. Їх застосування дає можливість перейти від формального дотримання положень до кількісного моніторингу, пріоритизації залишкового ризику та оцінювання стійкості коригувальних дій. Інтегральний індекс має використовуватися разом із переліком критичних винятків.

У сценарному тесті за сукупного властивого ризику 135 балів сукупний залишковий ризик після врахування результативності контролю та надійності доказу становив 47,84 бала, що відповідає скороченню на 64,56%. Найвищими залишилися ризики вторинного використання (11,00) та доступу (9,00). Розрахунок зрілості дав базове сценарне значення 42,50% та цільове 80,00%, а аналіз чутливості показав збільшення залишкового ризику з 5,00 до 13,00 за зниження D з 1,00 до 0,60. Це обґрунтовує окреме тестування як дизайну контролю, так і доказів його фактичного виконання.

Практичне впровадження методики доцільно здійснювати поетапно – від інвентаризації потоків і формування реєстру ключових контролів до пілотної автоматизованої аналітики, незалежного тестування та масштабування.

Удосконалено методичний підхід до внутрішнього контролю електронної медичної документації шляхом інтеграції контрольних цілей, ділянок життєвого циклу, контрольних процедур, системи доказів та індикаторів у єдину ризик-орієнтовану модель. На відміну від підходів, що окремо оцінюють якість даних, кібербезпеку або аудит-логи, запропонована модель передбачає коефіцієнт надійності контрольного доказу, який коригує номінальну результативність контролю та оцінку залишкового ризику. Практична цінність визначається можливістю застосувати методику для локальних політик, аудиторських програм, технічних вимог до MIC і управлінських панелей. Подальша емпірична апробація має встановити зв'язок між зрілістю контролю та клінічними, операційними й економічними результатами закладу. ■

БІБЛІОГРАФІЯ

1. Білошицька О. М., Бондаренко Л. В., Бесараб О. М. Проблеми та перспективи стандартизації електронної системи охорони здоров'я України. Ч. 1. Міжнародні стандарти з медичної інформатики. *Біомедична інженерія і технологія*. 2026. № 2. С. 99–116. DOI: https://doi.org/10.20535/.2026.2(22).359709

2. Holovachko V., Korolovich O., Havrylets O. Modern Transformations of Accounting, Management, and Marketing of an Enterprise in the Context of Digitalization. *Економіка та суспільство*. 2024. Вип. 66. DOI: https://doi.org/10.32782/2524-0072/2024-66-4
3. Постанова Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» від 25.04.2018 р. № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2018-п#Text
4. Наказ Міністерства охорони здоров'я України «Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я» від 28.02.2020 р. № 587. URL: https://zakon.rada.gov.ua/laws/show/z0236-20#Text
5. Електронна система охорони здоров'я. В ЕСОЗ кількість електронних медичних записів сягнула понад 5 млрд. 09.04.2026. URL: https://ehealth.gov.ua/2026/04/09/v-esoz-kilkist-elektronnyh-medychnyh-zapysiv-syagnula-ponad-5-mlrd/
6. Maksimova I. V. Regulation and organizational forms of internal audit of health care facilities. *Економіка, управління та адміністрування*. 2022. № 1. С. 69–75. DOI: https://doi.org/10.26642/ema-2022-1(99)-69-75
7. Закон України «Основи законодавства України про охорону здоров'я» від 19.11.1992 р. № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text
8. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
9. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
10. Сорока І. М., Кізім А. В., Мочалов Ю. О., Бобельський В. В., Комісар А. В. Аналіз проблем взаємодії операторів медичних інформаційних систем із самими системами на загальносвітовому рівні (огляд літератури). *Вісник соціальної гігієни та організації охорони здоров'я України*. 2025. № 4. С. 128–138. DOI: https://doi.org/10.11603/1681-2786.2025.4.15909
11. European Parliament and Council of the European Union. Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Official Journal of the European Union*. 2025. OJ L 2025/327, 5 March 2025. URL: https://eur-lex.europa.eu/eli/reg/2025/327/oj
12. Ghalavand H., Shirshahi S., Rahimi A., Zarrinabadi Z., Amani F. Common data quality elements for health information systems: a systematic review. *BMC Medical Informatics and Decision Making*. 2024. Vol. 24. Art. 243. DOI: https://doi.org/10.1186/s12911-024-02644-7
13. Huilgol Y. S., Adler-Milstein J., Ivey S. L., Hong J. C. Opportunities to use electronic health record audit logs to improve cancer care. *Cancer Medicine*. 2022. Vol. 11. Iss. 17. P. 3296–3303. DOI: https://doi.org/10.1002/cam4.4690
14. ISO 27799:2025. Health informatics – Information security controls in health based on ISO/IEC 27002. Geneva : International Organization for Standardization, 2025. URL: https://www.iso.org/standard/84647.html
15. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022. URL: https://www.iso.org/standard/27001
16. Lewis A. E., Weiskopf N., Abrams Z. B., et al. Electronic health record data quality assessment and tools: a systematic review. *Journal of the American Medical Informatics Association*. 2023. Vol. 30. Iss. 10. P. 1730–1740. DOI: https://doi.org/10.1093/jamia/ocad120
17. Palojoki S., Lehtonen L., Vuokko R. Semantic interoperability of electronic health records: systematic review of alternative approaches for enhancing patient information availability. *JMIR Medical Informatics*. 2024. Vol. 12. Art. e53535. DOI: https://doi.org/10.2196/53535
18. Rule A., Chiang M. F., Hribar M. R. Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods. *Journal of the American Medical Informatics Association*. 2020. Vol. 27. Iss. 3. P. 480–490. DOI: https://doi.org/10.1093/jamia/ocz196
19. The Institute of Internal Auditors. *Global Internal Audit Standards*. Iss. 9. January 2024. Effective 9 January 2025. URL: https://www.theiia.org/en/content/standards/complete-global-internal-audit-standards/

REFERENCES

Biloshytska O. M., Bondarenko L. V. & Besarab O. M. (2026). Problemy ta perspektyvy standartyzatsii elektronnoi systemy okhorony zdorovia Ukrainy. Ch. 1. Mizhnarodni standarty z medychnoi informatyky [Problems and prospects of standardization of the electronic health system of Ukraine. Part 1. International standards in medical informatics]. *Biomedychna inzheneriia i tekhnolohiia, 2* (22), 99–116. https://doi.org/10.20535/.2026.2(22).359709

Elektronna systema okhorony zdorovia. (2026, April 9). *V ESOZ kilkist elektronnykh medychnykh zapysiv siahnula ponad 5 mlrd* [In eHealth, the number of electronic medical records reached over 5 billion]. https://ehealth.gov.ua/2026/04/09/v-esoz-kilkist-elektronnyh-medychnyh-zapysiv-syagnula-ponad-5-mlrd/

European Parliament & Council of the European Union. (2025, March 5). Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2025/327/oj

Ghalavand H., Shirshahi S., Rahimi A., Zarrinabadi Z. & Amani F. (2024). Common data quality elements for health information systems: a systematic review. *BMC Medical Informatics and Decision Making, 24*(243). https://doi.org/10.1186/s12911-024-02644-7

Holovachko V., Korolovich O. & Havrylets O. (2024). Modern Transformations of Accounting, Management, and Marketing of an Enterprise in the Context of Digitalization. *Ekonomika ta suspilstvo, 66*. https://doi.org/10.32782/2524-0072/2024-66-4

Huilgol Y. S., Adler-Milstein J., Ivey S. L. & Hong J. C. (2022). Opportunities to use electronic health record audit logs to improve cancer care. *Cancer Medicine, 11*(17), 3296–3303. https://doi.org/10.1002/cam4.4690

The Institute of Internal Auditors. *Global Internal Audit Standards*. https://www.theiia.org/en/content/standards/complete-global-internal-audit-standards/

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001

International Organization for Standardization. (2025). *ISO 27799:2025. Health informatics – Information security controls in health based on ISO/IEC 27002*. https://www.iso.org/standard/84647.html

Lewis A. E., Weiskopf N. & Abrams Z. B. (2023). Electronic health record data quality assessment and tools: a systematic review. *Journal of the American Medical Informatics Association, 30*(10), 1730–1740. https://doi.org/10.1093/jamia/ocad120

Maksimova I. V. (2022). Regulation and organizational forms of internal audit of health care facilities. *Ekonomika, upravlinnia ta administruvannia, 1* (99), 69–75. https://doi.org/10.26642/ema-2022-1(99)-69-75

Palojoki S., Lehtonen L. & Vuokko R. (2024). Semantic interoperability of electronic health records: systematic review of alternative approaches for enhancing patient information availability. *JMIR Medical Informatics, 12*(e53535). https://doi.org/10.2196/53535

Rule A., Chiang M. F. & Hribar M. R. (2020). Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods. *Journal of the American Medical Informatics Association, 27*(3), 480–490. https://doi.org/10.1093/jamia/ocz196

Soroka I. M., Kizim A. V., Mochalov Yu. O., Bobelskyi V. V. & Komisar A. V. (2025). Analiz problem vzaiemodii operatoriv medychnykh informatsiinykh system iz samymy systemamy na zahalnosvitovomu rivni (ohliad literatury) [Analysis of the problems of interaction between operators of medical information systems and the systems themselves at the global level (literature review)]. *Visnyk sotsialnoi hihiieny ta orhanizatsii okhorony zdorovia Ukrainy, 4*, 128–138. https://doi.org/10.11603/1681-2786.2025.4.15909

zakon.rada.gov.ua. (1992, November 19). Zakon Ukrainy «Osnovy zakonodavstva Ukrainy pro okhoronu zdorovia» vid 19.11.1992 r. № 2801-XII [Law of Ukraine "Fundamentals of Health Legislation of Ukraine" dated November 19, 1992 No. 2801-XII]. https://zakon.rada.gov.ua/laws/show/2801-12#Text

zakon.rada.gov.ua. (2003, May 22). Zakon Ukrainy «Pro elektronni dokumenty ta elektronnyi dokumentoobih» vid 22.05.2003 r. № 851-IV [Law of Ukraine "On Electronic Documents and Electronic Document Circulation" dated May 22, 2003 No. 851-IV]. https://zakon.rada.gov.ua/laws/show/851-15#Text

zakon.rada.gov.ua. (2010, June 1). Zakon Ukrainy «Pro zakhyst personalnykh danykh» vid 01.06.2010 r. № 2297-VI [Law of Ukraine "On Personal Data Protection" dated June 1, 2010 No. 2297-VI]. https://zakon.rada.gov.ua/laws/show/2297-17#Text

zakon.rada.gov.ua. (2018, April 25). Postanova Kabinetu Ministriv Ukrainy «Deiaki pytannia elektronnoi systemy okhorony zdorovia» vid 25.04.2018 r. № 411 [Resolution of the Cabinet of Ministers of Ukraine "Some issues of the electronic health system" dated April 25, 2018 No. 411]. https://zakon.rada.gov.ua/laws/show/411-2018-p#Text

zakon.rada.gov.ua. (2020, February 28). Nakaz Ministerstva okhorony zdorovia Ukrainy «Deiaki pytannia vedennia Reiestru medychnykh zapysiv, zapysiv pro napravlennia ta retseptiv v elektronnii systemi okhorony zdorovia» vid 28.02.2020 r. № 587 [Order of the Ministry of Health of Ukraine "Some issues of keeping the Register of medical records, referral records and prescriptions in the electronic health system" dated February 28, 2020 No. 587]. https://zakon.rada.gov.ua/laws/show/z0236-20#Text

Дослідження не отримувало зовнішнього фінансування.

Автори заявляють про відсутність конфлікту інтересів.

Під час перевірки та доопрацювання рукопису автори використовували інструмент OpenAI ChatGPT у режимі Codex, модель і версія – GPT-5.6 Sol. Інструмент застосовувався для допоміжної перевірки логічної узгодженості та структури тексту, виявлення повторів, мовностилістичного редагування й підготовки варіантів окремих формулювань. Усі отримані пропозиції та матеріали були критично перевірені, відредаговані й остаточно схвалені авторами. Автори несуть повну відповідальність за достовірність наведених даних, точність посилань, наукові положення, висновки та остаточний зміст рукопису.

Стаття надійшла до редакції / Received: 28.08.2026
Статтю прийнято до публікації / Accepted: 10.09.2026
Оприлюднено / Published: 19.10.2026