КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1004
УДК 004.056.5

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Кія Олексій Сергійович
магістрант Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0003-4105-8081
oskiia.fitm24m@kubg.edu.ua

НАПІВАВТОМАТИЗОВАНИЙ ІНСТРУМЕНТ БАГАТОСТАНДАРТНОЇ ОЦІНКИ КІБЕРЗРІЛОСТІ ОРГАНІЗАЦІЇ НА ОСНОВІ NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 ТА CIS CONTROLS V8

Анотація. У сучасному ландшафті кіберзагроз жоден програмний таф технічний засіб не може повністю компенсувати відсутність комплексного підходу до управління безпекою, що включає як технологічні, так і організаційні аспекти. Сучасні організації часто змушені відповідати вимогам декількох міжнародних стандартів одночасно (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) через регуляторні зобов'язання, вимоги клієнтів та внутрішні політики, що призводить до фрагментації зусиль, дублювання робіт та неефективного використання обмежених ресурсів. Дана стаття присвячена розробці напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості, який дозволяє організаціям провести оцінку відповідності всім чотирьом фреймворкам через єдину точку входу — структуроване опитування за фреймворком NIST CSF 2.0 як базового вимірювального інструменту, COBIT 2019 як механізму визначення цільового стану через пріоритизацію бізнес-процесів, ISO/IEC 27001:2022 як референсу документованих контролів та CIS Controls v8 як додаткової практичної деталізації для малих та середніх організацій (МСО). На основі систематичного аналізу наукової літератури та практичних кейсів обґрунтовано необхідність використання матриці відповідностей (mapping matrix) між стандартами для автоматичного відображення результатів оцінки у термінах всіх чотирьох фреймворків одночасно. Описано архітектуру інструменту та деталізовано логіку його роботи: від формування експертної групи та збору організаційного контексту до автоматизованого оцінювання поточного стану та генерації рекомендацій для цільового. Науковою новизною роботи є розробка практичного інструменту, що поєднує методологічні підходи, а саме: багатостандартну оцінку кіберзрілості організації через матрицю відповідностей між NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8, яка дозволяє уникнути дублювання зусиль при відповідності множинним стандартам; напівавтоматизацію оцінки з використанням об'єктивних структурованих опитувальників, що підвищує надійність та повторюваність результатів; валідацію результатів міждисциплінарною експертною групою за принципом «Human-in-the-Loop», що забезпечує

врахування організаційного контексту. Охарактеризовано роль експертної групи як валідатора автоматично згенерованих даних та визначника організаційних пріоритетів, що дозволяє поєднати переваги автоматизації з гнучкістю експертного аналізу. Особливу увагу приділено економічній ефективності запропонованого рішення через використання загальнодоступних інструментів (Microsoft Excel) та можливості поетапного впровадження для МСО через систему груп впровадження CIS Controls (IG1→IG2→IG3).
Результати дослідження можуть бути використані як практичний інструмент для організацій будь-якого розміру: малі організації можуть розпочати з базового рівня (CIS IG1) та поступово нарощувати зрілість, тоді як великі підприємства отримують комплексний огляд відповідності множинним стандартам через єдину модель оцінки без дублювання зусиль.

Ключові слова: кіберзрілість; багатостандартна оцінка; NIST CSF 2.0; ISO/IEC 27001:2022; COBIT 2019; CIS Controls v8; напівавтоматизована оцінка; експертна група; матриця відповідностей; дорожня карта

ВСТУП

Постановка проблеми. Сучасний ландшафт інформаційної безпеки характеризується безпрецедентним зростанням кількості та складності кіберзагроз. За даними IBM Cost of a Data Breach Report 2025 середня глобальна вартість витоку даних становить 4,44 мільйона доларів США, тоді як у Сполучених Штатах цей показник досягає рекордних 10,22 мільйона доларів [1]. Згідно з прогнозами Cybersecurity Ventures, глобальні збитки від кіберзлочинності у 2025 році становлять 10,5 трильйона доларів США [2].

Особливо вразливими є малі та середні організації (МСО). Дослідження 2024-2025 років засвідчують, що 94% МСО зазнали щонайменше однієї кібератаки протягом 2024 року, при цьому 78% висловлюють занепокоєння можливістю припинення діяльності внаслідок витоку даних [3]. У Великій Британії 41% мікропідприємств та 50% малих підприємств ідентифікували порушення безпеки або атаки у 2025 році [4]. Критичною є статистика, згідно з якою 60% малих підприємств закривають свою діяльність протягом шести місяців після серйозного інциденту кібербезпеки [5].

У відповідь на зростаючі виклики провідні міжнародні організації розробили численні фреймворки, кожен з яких пропонує унікальний підхід до оцінки та управління кіберризиками. Серед найбільш впливових слід виділити NIST Cybersecurity Framework (CSF), ISO/IEC 27001, COBIT 2019 та CIS Critical Security Controls [6-8]. NIST CSF 2.0, оновлений у лютому 2024 року, забезпечує гнучкий, ризик-орієнтований підхід через шість ключових функцій: Govern, Identify, Protect, Detect, Respond та Recover [9-10]. Систематичний огляд 2024-2025 років підтверджує широке визнання та застосування NIST CSF у різних секторах. CIS Controls v8, оновлені до версії 8.1 у червні 2024 року Центром інтернет-безпеки (Center for Internet Security), надають практично орієнтований набір із 18 контролів та 153 заходи безпеки, пріоритизованих через систему груп впровадження (Implementation Groups), що робить їх особливо доступними для МСО [11-12].

Проте жоден із фреймворків не є універсальним рішенням для всіх організацій [13-14]. Сучасні організації часто змушені відповідати вимогам декількох стандартів одночасно через регуляторні зобов'язання, вимоги клієнтів та внутрішні політики [15]. Наприклад, фінансові установи можуть бути зобов'язані дотримуватися NIST CSF для відповідності федеральним вимогам США, ISO 27001 для міжнародної сертифікації, COBIT для управління IT-ризиками на рівні ради директорів, та CIS Controls для практичного впровадження технічних заходів. Це призводить до фрагментації зусиль,

дублювання робіт та неефективного використання обмежених ресурсів, оскільки кожен стандарт зазвичай оцінюється окремо, незважаючи на значне перекриття їхніх вимог.

Ключовою проблемою для МСО є те, що більшість існуючих інструментів оцінки кіберзрілості розроблені для великих корпорацій з відповідними бюджетами, кваліфікованим персоналом та розвиненою інфраструктурою безпеки [16-17]. За даними звіту PwC Global Digital Trust Insights 2025, лише 2% компаній у світі вважають себе повністю стійкими до кіберзагроз, при цьому 66% керівників технологічних підрозділів визначають кібербезпеку як головний бізнес-ризик [18]. Навіть, коли МСО прагнуть впровадити міжнародні стандарти, вони стикаються з бар'єром входу: складність документації ISO 27001, абстрактність результатів NIST CSF, управлінський фокус COBIT часто перевищують можливості невеликих команд без спеціалізованих знань [19-20]. Крім того, проведення окремих оцінок за кожним стандартом вимагає значних часових та фінансових витрат, які МСО не можуть собі дозволити

Додатковим викликом є суб'єктивність традиційних підходів до оцінки кіберзрілості, що може призводити до завищення або заниження реального стану безпеки організації [21-22]. Систематичний огляд 2024 року виявив, що більшість існуючих моделей зрілості кібербезпеки (CCMMs) страждають від обмеженості в охопленні безпеки та відсутності кількісних метрик, що ускладнює їх впровадження та призводить до фрагментованих оцінок [23].

Отже, існує нагальна потреба у розробці доступного та економічно ефективного інструменту багатостандартної оцінки кіберзрілості, який дозволяє організаціям через єдину точку входу отримати оцінку відповідності всім чотирьом провідним міжнародним фреймворкам (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) без дублювання зусиль. Такий інструмент має забезпечувати об'єктивність оцінювання через структуровані опитувальники, дозволяти визначати цільовий стан на основі бізнес-пріоритетів організації, автоматично відображати результати у термінах всіх стандартів одночасно, та бути адаптованим до потреб малих та середніх організацій. Інструмент має базуватися на принципах напівавтоматизації, де технологічні рішення доповнюються експертним судженням за принципом «Human-in-the-Loop», дозволяючи знизити вартість впровадження при збереженні високої якості оцінки.

Аналіз останніх досліджень і публікацій.

Доступні рішення для малих та середніх організацій. Curtin та Moran (2024) у дослідженні для малих ірландських підприємств виявили ключову проблему традиційних підходів до оцінки кібербезпеки: більшість методологій вимагають глибоких технічних знань та значних часових ресурсів, що робить їх недоступними для МСО [24]. У відповідь вони розробили веб-інструмент, який дозволяє власникам малого бізнесу без спеціалізованих знань провести самооцінку кіберризиків за 10 хвилин. Ключовою інновацією їхнього підходу є автоматична генерація персоналізованого плану дій на основі об'єктивних відповідей на структуровані питання. Це усуває головну проблему традиційних методів самооцінки — суб'єктивність, коли організації схильні переоцінювати або недооцінювати свій рівень захищеності. Автори довели, що використання об'єктивних індикаторів (наприклад, «чи існує задокументована політика?» замість «чи вважаєте ви свою політику адекватною?») підвищує точність оцінки та забезпечує порівнянність результатів між різними організаціями.

Автори [25] запропонували модель управління ризиками інформаційної безпеки для МСО на основі використання якісного та кількісного підходів до оцінки ризиків. Змістова лінія моделі акцентує увагу на покрокове проведення SWOT-аналізу для швидкої ідентифікації ризиків; застосування статистичного методу, якщо існує база

аналітичних даних, у протилежному випадку – метод експертних оцінок; метод Монте-Карло.

Моделювання інформаційних ризиків малого бізнесу було представлено у дослідженні [26]. Науковці розробили опитувальник для експертів з використанням SWOT-аналізу, в результаті якого виділено сім ключових загроз (від зовнішніх атак до непередбачених змін) та шість уразливостей (відсутність резервного копіювання, плинність кадрів тощо). Оцінки узгодили коефіцієнтом конкордації Кендалла та обробили методом попарних порівнянь в Excel, що дозволило побудувати порівняльну матрицю загроз і уразливостей для прийняття управлінських рішень.

Європейське агентство з кібербезпеки (ENISA) у 2024 році опублікувало оновлений інструмент оцінки кіберзрілості для МСО, який також підкреслює важливість об'єктивних, вимірюваних індикаторів [20].

Багатостандартна оцінка як шлях до ефективності. Мета-аналіз 2025 року, опублікований у Journal of Strategic Defense and Policy Studies, охопив 78 рецензованих досліджень та галузевих звітів за період 2010-2024 років і надав переконливі емпіричні докази переваг багатостандартної оцінки [27]. Дослідники виявили, що організації, які використовують інструменти для паралельної оцінки відповідності множинним фреймворкам кібербезпеки (NIST CSF, ISO 27001, COBIT) у свої системи управління ризиками та відповідності (GRC), демонструють статистично значущі покращення порівняно з організаціями, що проводять окремі оцінки за кожним стандартом: скорочення середнього часу виявлення та локалізації інцидентів безпеки на 34%, зменшення кількості порушень регуляторної відповідності на 41%, підвищення готовності до зовнішніх аудитів на 52%, зниження витрат на відповідність множинним стандартам на 43% через уникнення дублювання зусиль

Sulistyowati та співавтори (2020) конкретизували механізм багатостандартної оцінки, запропонувавши матрицю відповідностей (cross-reference matrix), яка встановлює семантичні зв'язки між контролями різних стандартів [28]. Їхнє емпіричне дослідження показало, що така матриця не лише знижує адміністративне навантаження через уникнення дублювання зусиль, але й забезпечує більш цілісне розуміння стану кібербезпеки. Організація може провести одну оцінку за базовим фреймворком, а потім через матрицю відповідностей автоматично отримати результати у термінах інших стандартів. Центр інтернет-безпеки (CIS) у червні 2024 року опублікував офіційний маппінг між CIS Controls v8.1 та NIST CSF 2.0, що встановлює чіткі відповідності між 153 заходи безпеки CIS та 106 субкатегоріями NIST CSF [29]. Цей офіційний документ демонструє, що використання матриці відповідностей між практично орієнтованими діями CIS та стратегічними результатами NIST створює дорожню карту впровадження для МСО, яка чітко вказує, з яких конкретних кроків розпочати захист, одночасно відслідковуючи відповідність вимогам NIST CSF.

Роль експертних груп та напівавтоматизація оцінки. Yousaf та Khan (2025) у дослідженні напівавтоматизованої моделі «STPA-Cyber» продемонстрували обмеження як повністю автоматизованих, так і повністю ручних підходів до оцінки кібербезпеки [30]. Повністю автоматизовані системи, хоча й забезпечують об'єктивність та масштабованість, часто не враховують організаційний контекст, специфіку бізнес-процесів та стратегічні цілі конкретної організації. З іншого боку, повністю ручні оцінки схильні до суб'єктивності та непослідовності. Їхнє рішення — підхід «Human-in-the-Loop», де структуровані опитувальники забезпечують автоматизований збір об'єктивних доказів стану безпеки, але експертна група зберігає право валідувати результати,

коригувати оцінки з урахуванням специфіки організації та адаптувати рекомендації до реальних можливостей впровадження.

«Ontario Cyber Security Expert Panel» (2022) конкретизував роль експертних груп у контексті багатостандартної оцінки, рекомендуючи створення міждисциплінарних команд, які включають представників IT-підрозділу, інформаційної безпеки, юридичного відділу та ключових бізнес-підрозділів [31]. Така експертна група виконує три критично важливі функції:

1) формування організаційного контексту та визначення пріоритетів для багатостандартної оцінки на основі стратегічних цілей та операційних реалій організації;
2) валідація автоматизованих результатів оцінки через перевірку їх відповідності фактичному стану справ у всіх чотирьох фреймворках;
3) адаптація рекомендацій щодо покращень до специфіки організації, її ресурсних обмежень та пріоритетів, визначаючи, які стандарти є найбільш критичними для конкретної організації.

ISACA у 2024 році опублікувала керівництво щодо застосування моделі трьох ліній захисту (Three Lines Model) у контексті управління кібербезпекою та ризиками, де експертна група представляє другу лінію захисту — функцію нагляду та експертизи [32].

Водночас, залишається невирішеним питання створення практичного інструменту багатостандартної оцінки, який би органічно поєднував:

- доступність для МСО через використання об'єктивних структурованих опитувальників та економічно ефективної реалізації у загальнодоступних інструментах (Microsoft Excel);
- багатостандартну оцінку відповідності чотирьом провідним фреймворкам (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) через єдину точку входу з використанням матриці відповідностей для автоматичного відображення результатів у термінах всіх стандартів;
- напівавтоматизацію процесів gap-аналізу та формування дорожніх карт покращень з обов'язковою експертною валідацією за принципом «Human-in-the-Loop».

Мета статті. Метою статті є розробка та обґрунтування напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості організації, що базується на провідних міжнародних фреймворках NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8, з акцентом на доступності та економічній ефективності рішення для малих та середніх організацій.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати чотири провідні фреймворки кібербезпеки (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) для обґрунтування їх використання у багатостандартній оцінці, ідентифікувати їх комплементарність та специфічні ролі у запропонованому інструменті.

2. Розробити методологію побудови матриці відповідностей між 106 субкатегоріями NIST CSF 2.0, 93 контролями ISO/IEC 27001:2022 Додатку A, 40 цілями управління COBIT 2019 та 153 заходами безпеки CIS Controls v8, яка дозволяє автоматично відображати результати оцінки за базовим фреймворком NIST CSF у термінах інших трьох стандартів.

3. Обґрунтувати роль експертної групи у процесі багатостандартної оцінки кіберзрілості як ключового механізму валідації автоматизованих результатів, визначення

організаційних пріоритетів, адаптації рекомендацій до організаційного контексту та забезпечення принципу «Human-in-the-Loop».

4. Розробити архітектуру напівавтоматизованого інструменту багатостандартної оцінки, що включає: а) модуль структурованого опитування за NIST CSF 2.0 з автоматичним присвоєнням оцінок зрілості (0-5); б) модуль матриці відповідностей для автоматичного відображення результатів у термінах ISO 27001, COBIT та CIS Controls; в) модуль експертної валідації результатів; г) модуль «gap-аналізу» та формування дорожньої карти покращень одночасно для всіх чотирьох фреймворків.

5. Описати чотирифазну методологію роботи з інструментом: 1) формування експертної групи та визначення організаційного контексту; 2) оцінка поточного стану (As-Is) через структуроване опитування за NIST CSF з автоматичним відображенням відповідності ISO 27001, COBIT та CIS Controls; 3) визначення цільового стану (To-Be) на основі бізнес-пріоритетів через структуру COBIT з автоматичним формуванням цільового профілю у термінах NIST CSF; 4) автоматичний gap-аналіз та генерація дорожньої карти покращень одночасно для всіх чотирьох фреймворків.

6. Продемонструвати практичну реалізацію інструменту у вигляді доступного рішення в середовищі Microsoft Excel для забезпечення економічної ефективності та простоти використання малими та середніми організаціями, з можливістю поетапного впровадження.

Результати дослідження можуть бути використані організаціями для самооцінки та підвищення рівня кіберзрілості через єдину багатостандартну оцінку, консультантами з кібербезпеки для проведення аудитів відповідності множинним стандартам без дублювання зусиль, а також в якості навчального матеріалу для студентів спеціальності «Кібербезпека та захист інформації».

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Становлення сучасних підходів до оцінки кіберзрілості організацій стало можливим завдяки багаторічній еволюції міжнародних стандартів та фреймворків, які відображають накопичений досвід, кращі практики та вимоги до захисту інформаційних активів у різних секторах економіки. Серед найбільш впливових і поширених у світі слід виділити NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8. Кожен з цих стандартів має унікальний фокус, цільову аудиторію та методологію, що робить їх комплементарними при використанні для багатостандартної оцінки кіберзрілості [6-8, 11].

NIST Cybersecurity Framework 2.0 був оновлений у лютому 2024 року та представляє собою гнучкий, ризик-орієнтований підхід до управління кіберризиками [9]. Ключовою інновацією версії 2.0 стало введення нової функції Govern (Управління), яка доповнила п'ять існуючих функцій: Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування) та Recover (Відновлення) [12]. Структура фреймворку побудована ієрархічно: 6 функцій деталізуються через 23 категорії, які, у свою чергу, конкретизуються через 106 субкатегорій, кожна з яких описує конкретний результат (outcome), який організація має досягти [9]. Важливою особливістю NIST CSF є його технологічна нейтральність — фреймворк застосовується до всіх типів ІКТ, включаючи традиційні інформаційні технології, Інтернет речей, операційні технології, хмарні середовища та системи штучного інтелекту [9].

ISO/IEC 27001:2022 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), оновленим у жовтні 2022 року [33]. На відміну від

NIST CSF, який є добровільним фреймворком, ISO 27001 є нормативним стандартом, що дозволяє організаціям отримати офіційну міжнародну сертифікацію [8]. Структура стандарту складається з основних положень (Розділи 4-10), які описують вимоги до побудови ISMS, та Додатку А, який містить 93 контролі безпеки, згруповані за чотирма тематичними категоріями: організаційні контролі (37), контролі персоналу (8), фізичні контролі (14) та технологічні контролі (34) [33-34]. Порівняно з попередньою версією 2013 року, кількість контролів зменшилася зі 114 до 93 через об'єднання дублюючих контролів та введення 11 нових контролів для вирішення сучасних викликів кібербезпеки [33-34].

COBIT 2019 (Control Objectives for Information and Related Technologies) є комплексним фреймворком для управління та врядування інформаційних технологій, випущеним ISACA у квітні 2019 року [35-36]. На відміну від NIST CSF та ISO 27001, які зосереджені безпосередньо на кібербезпеці, COBIT має ширший фокус на вирівнюванні IT-стратегії з бізнес-цілями організації. Структура COBIT організована навколо п'яти доменів: один домен управління (Evaluate, Direct and Monitor) та чотири домени менеджменту (Align, Plan and Organize; Build, Acquire and Implement; Deliver, Service and Support; Monitor, Evaluate and Assess). Фреймворк містить 40 цілей управління та врядування, кожна з яких деталізує конкретні процеси, організаційні структури, потоки інформації та необхідні компетенції персоналу [35-36].

CIS Controls v8 (Center for Internet Security Critical Security Controls), оновлені до версії 8.1 у червні 2024 року, являють собою практично орієнтований набір із 18 контролів безпеки, деталізованих через 153 заходи безпеки [11, 37]. Унікальною особливістю CIS Controls є їх пріоритизація через систему Implementation Groups (IGs), яка дозволяє організаціям різного розміру та зрілості поступово впроваджувати контролі: IG1 (56 safeguards) призначений для малих організацій з обмеженими ресурсами, IG2 (додаткові 74 safeguards) — для середніх організацій, IG3 (додаткові 23 safeguards) — для великих підприємств з експертами безпеки [12, 38-39]. Версія 8.1 внесла важливі оновлення для вирівнювання з NIST CSF 2.0, включаючи введення нової категорії активів "Documentation" та security function "Governance" [40].

Порівняльний аналіз цих чотирьох фреймворків демонструє їх комплементарність. Таблиця 1 систематизує ключові характеристики кожного стандарту.

Таблиця 1.

Порівняльний аналіз провідних фреймворків кібербезпеки

Критерій	**NIST CSF 2.0**	**ISO/IEC 27001:2022**	**COBIT 2019**	**CIS Controls v8**
Версія	2.0	27001:2022	2019	v8.1 (2024)
Рік випуску	Лютий 2024	Жовтень 2022	Квітень 2019	Червень 2024
Основний фокус	Ризик-орієнтоване управління кіберризиками	Система управління інформаційною безпекою	Управління IT та вирівнювання бізнес-IT	Практичні дії для захисту від кіберзагроз
Структура	6 функцій → 23 категорії → 106 субкатегорій	Розділи 4-10 + Додаток А (93 контролі)	5 доменів → 40 цілей управління	18 контролів → 153 заходи безпеки → 3 групи впровадження
Кількість елементів	106 субкатегорій	93 контролі в Додатку А	40 цілей управління та врядування	153 заходи безпеки

Критерій	NIST CSF 2.0	ISO/IEC 27001:2022	COBIT 2019	CIS Controls v8
Гнучкість	Висока (адаптивний фреймворк)	Середня (вимагає дотримання структури)	Висока (11 факторів налаштування)	Висока (3 рівні груп впровадження)
Сертифікація	Ні (добровільний фреймворк)	Так (міжнародна сертифікація)	Ні (рамковий стандарт)	Ні (набір найкращих практик)
Цільова аудиторія	Будь-які організації (уряд, бізнес, МСО)	Організації, що потребують сертифікації	IT-департаменти, директори з інформатизації	МСО з обмеженими ресурсами
Підхід	Стратегічний, орієнтований на результати	Процесний, орієнтований на вимоги	Управлінський, орієнтований на врядування	Практичний, орієнтований на дії
Основні переваги	Гнучкість, універсальність, широке визнання	Міжнародне визнання, сертифікація	Вирівнювання бізнесу та IT, метрики	Простота впровадження, орієнтація на МСО
Основні обмеження	Відсутність сертифікації, потребує адаптації	Вартість сертифікації, жорсткість структури	Складність впровадження, потребує зрілості	Менша деталізація для складних середовищ

Жоден із зазначених стандартів не є універсально найкращим. NIST CSF забезпечує стратегічну гнучкість та ризик-орієнтований підхід. ISO/IEC 27001 надає формалізацію процесів та можливість міжнародної сертифікації ISMS. COBIT забезпечує стратегічний зв'язок бізнесу й IT через детальну оцінку зрілості процесів. CIS Controls пропонують практичні, пріоритизовані дії, особливо цінні для МСО з обмеженими ресурсами [6-8, 11].

Ключовим викликом у розробці інструменту оцінки кіберзрілості є знаходження балансу між автоматизацією та експертним судженням. Повністю автоматизовані системи, хоча й забезпечують об'єктивність та масштабованість, часто не враховують організаційний контекст та специфіку бізнес-процесів [30]. З іншого боку, повністю ручні оцінки схильні до суб'єктивності та непослідовності [21-22].

Концепція “Human-in-the-Loop” пропонує оптимальне рішення цієї дилеми. Дослідження показують, що напівавтоматизований підхід, де структуровані об'єктивні опитувальники забезпечують автоматизований збір доказів стану безпеки, але експертна група зберігає право валідувати результати та адаптувати рекомендації до специфіки організації, дозволяє досягти балансу між об'єктивністю та контекстуальністю [30]. Європейське агентство з кібербезпеки (ENISA) у 2024 році підкреслило важливість об'єктивних, вимірюваних індикаторів у інструментах самооцінки для МСО [20].

Об'єктивні опитувальники відрізняються від суб'єктивних формулюванням питань. Наприклад, замість суб'єктивного питання "Чи вважаєте ви вашу політику безпеки адекватною?" використовується об'єктивне: "Чи існує задокументована, затверджена керівництвом політика інформаційної безпеки, яка була переглянута протягом останніх 12 місяців?" [24]. Така формулювання дозволяє отримати перевірену відповідь та забезпечує порівнянність результатів між різними організаціями.

Структура об'єктивного опитувальника для кожної субкатегорії NIST CSF включає серію питань, які поступово деталізують стан впровадження контролю. На основі відповідей система автоматично присвоює оцінку зрілості за шкалою 0-5, де 0 означає повну відсутність контролю, 1 — початковий рівень, 2 — повторюваний, 3 —

визначений/документований, 4 — керований/вимірюваний, 5 — оптимізований з постійним вдосконаленням. Така шкала відповідає широко визнаним моделям зрілості, таким як Capability Maturity Model Integration (CMMI) [41].

Таким чином, теоретичною основою розробленого інструменту є інтеграція чотирьох комплементарних фреймворків кібербезпеки (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) через напівавтоматизований підхід, що поєднує об'єктивні структуровані опитувальники з експертною валідацією за принципом «Human-in-the-Loop». Це забезпечує надійну, повторювану та контекстуально релевантну оцінку кіберзрілості організацій різного розміру та складності

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результатом проведеного дослідження є розробка напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості організації, який поєднує провідні міжнародні фреймворки кібербезпеки. Інструмент надає механізм паралельної оцінки відповідності організації вимогам NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8 через єдину точку входу — структуроване опитування за базовим фреймворком NIST CSF 2.0.

Архітектура напівавтоматизованого інструменту оцінки кіберзрілості

NIST CSF 2.0 виконує роль базового вимірювального інструменту. Організація проходить структуроване опитування за всіма 106 субкатегоріями NIST CSF, що забезпечує комплексний огляд стану кібербезпеки за шістьма ключовими функціями: Govern, Identify, Protect, Detect, Respond, Recover. Кожна субкатегорія оцінюється за шкалою зрілості 0-5, де автоматизований алгоритм присвоює оцінку на основі об'єктивних відповідей на структуровані питання [9, 24].

ISO/IEC 27001:2022 виконує роль референсу документованих контролів. Через матрицю відповідностей між субкатегоріями NIST CSF та контролями ISO 27001 Додаток А інструмент автоматично відображає, яким вимогам ISO організація відповідає на основі оцінки за NIST CSF. Це особливо важливо для організацій, які мають або планують отримати сертифікацію ISO 27001, оскільки дозволяє побачити стан відповідності без проведення окремого аудиту [33-34].

COBIT 2019 виконує роль механізму пріоритизації та визначення цільового стану. Експертна група організації використовує структуру COBIT для систематичного аналізу стратегічних пріоритетів, критичних бізнес-процесів та ресурсних можливостей. На основі цього аналізу визначаються пріоритетні цілі управління COBIT, які через матрицю відповідностей автоматично транслюються у цільовий профіль зрілості у термінах NIST CSF [35-36]. Такий підхід забезпечує, що цільовий стан кіберзрілості не є абстрактним «максимальним захистом», а реалістичним профілем, який відповідає бізнес-потребам організації.

CIS Controls v8 виконує роль додаткової практичної деталізації для МСО. Для субкатегорій NIST CSF розроблено комплексний маппінг до CIS Controls, який базується на офіційному маппінгу з авторським доопрацюванням для функцій Govern, Respond та Recover. Інструмент автоматично показує відповідні safeguards з указанням Implementation Group (IG1/IG2/IG3) [29]. Це дозволяє МСО отримати конкретні, пріоритизовані технічні дії для впровадження.

Компонентна структура інструменту включає п'ять ключових модулів:

Модуль 1: Формування експертної групи та організаційного контексту. На початковому етапі формується міждисциплінарна експертна група, яка включає

представників IT-підрозділу, інформаційної безпеки, юридичного відділу, служби управління ризиками та ключових бізнес-підрозділів [31]. Експертна група проводить структуроване обговорення стратегічних цілей організації, критичних бізнес-процесів, профілю ризиків, регуляторних вимог та наявних ресурсів, результати якого фіксуються в документі "Організаційний контекст".

Модуль 2: Оцінка поточного стану (As-Is) за NIST CSF 2.0. Організація проходить структуроване опитування, яке охоплює всі 106 субкатегорій NIST CSF. Для кожної субкатегорії опитувальник містить серію об'єктивних питань, які дозволяють системі автоматично присвоїти оцінку зрілості 0-5. Після завершення опитування експертна група проводить валідацію результатів, перевіряючи їх відповідність фактичному стану справ та за необхідності коригуючи оцінки з урахуванням організаційного контексту [30].

Модуль 3: Визначення цільового стану (To-Be) через COBIT 2019. Експертна група використовує структуру COBIT для визначення пріоритетних цілей управління в кожному з п'яти доменів. Ці цілі через матрицю відповідностей автоматично транслюються у цільові значення зрілості для відповідних субкатегорій NIST CSF, формуючи цільовий профіль. Наприклад, якщо організація визначає високий пріоритет для процесу COBIT DSS05 "Manage Security Services", інструмент автоматично встановлює цільову зрілість 4-5 для відповідних субкатегорій NIST CSF функції Protect [35-36].

Модуль 4: Матриця відповідностей та багатостандартне відображення. Після оцінки за NIST CSF інструмент через матрицю відповідностей автоматично відображає результати у термінах інших трьох фреймворків. Для кожної субкатегорії NIST система показує: відповідні контролі ISO 27001 Додатку A з короткими описами; відповідні процеси COBIT з доменами; відповідні контролі CIS з групи імплементації [28-29, 33, 35].

Модуль 5: Gap-аналіз та формування дорожньої карти покращень. Інструмент автоматично порівнює поточний стан (As-Is) та цільовий стан (To-Be) для кожної субкатегорії NIST CSF, ідентифікуючи прогалини (gaps). На основі gap-аналізу формується дорожня карта покращень, яка містить конкретні рекомендації одночасно у термінах всіх чотирьох фреймворків: які субкатегорії NIST CSF потребують підвищення зрілості, які контролі ISO 27001 необхідно впровадити або покращити, які контролі CIS рекомендовані для впровадження. Експертна група адаптує цю дорожню карту, враховуючи ресурсні обмеження, пріоритетність бізнес-процесів та реалістичні терміни впровадження [27, 31].

Методологія побудови матриці відповідностей між фреймворками

Реалізація багатостандартної оцінки вимагає створення матриці відповідностей (mapping matrix) між елементами чотирьох фреймворків. Ця матриця дозволяє, оцінюючи організацію за базовим фреймворком NIST CSF 2.0, автоматично відображати результати у термінах ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8.

Методологія побудови матриці відповідностей включає п'ять послідовних етапів:

Етап 1: Аналіз офіційних маппінгів. Відправною точкою є систематичний аналіз офіційних документів NIST, CIS та ISACA, які встановлюють відповідності між фреймворками [9, 29, 42].

Етап 2: Семантичний аналіз елементів фреймворків. Для кожної субкатегорії NIST CSF 2.0 проводиться детальний аналіз її опису, мети та очікуваних результатів. Паралельно аналізуються контролі ISO/IEC 27001:2022 Додатку A та цілі управління COBIT 2019 для ідентифікації відповідностей. Семантичний аналіз показав, що всі 106

субкатегорій NIST CSF мають щонайменше одну відповідність в ISO 27001 та COBIT, що підтверджує повноту покриття цих двох стандартів [33, 35].

Етап 3: Формалізація матриці у реляційній структурі. Результати попередніх етапів формалізуються у вигляді реляційної таблиці, де кожен запис містить: ідентифікатор та опис субкатегорії NIST CSF 2.0; список відповідних контролів ISO/IEC 27001:2022 Додатку А; список відповідних цілей управління COBIT 2019; список відповідних контролів CIS v8 [28-29].

Етап 4: Офіційний маппінг CIS → NIST CSF було доопрацьовано авторами для кращої сумісності фреймворків CIS і NIST CSF [29].

Приклад матриці відповідностей для кількох репрезентативних субкатегорій NIST CSF 2.0 представлено в таблиці 2.

Таблиця 2.

Приклад матриці відповідностей між NIST CSF 2.0 та іншими фреймворками

NIST CSF 2.0	Опис	ISO 27001:2022	COBIT 2019	CIS Controls v8
ID.AM-01	Фізичні пристрої та системи інвентаризовані	A.5.9	BAI09	1.1 (IG1)
PR.DS-02	Дані в русі захищені	A.5.3; A.8.2; A.8.17; A.8.20; A.8.22	APO01, DSS05, DSS06	3.1 (IG1)
DE.CM-01	Мережі та середовище моніторяться	A.8.16	DSS01, DSS03, DSS05	13.1 (IG1)
RS.MA-01	Інциденти класифіковані та задокументовані	A.5.26; A.5.27	APO12, DSS03	17.4 (IG2)

Запропонований формат для матриці відповідності стане в основу майбутньої логіки роботи інструменту.

Чотирифазний процес оцінки кіберзрілості

Робота з інструментом організована у вигляді чотирифазного процесу, який забезпечує послідовне проходження від формування контексту до отримання практичних рекомендацій.

Фаза 1: Формування організаційного контексту та експертної групи. На початковому етапі організація формує міждисциплінарну експертну групу та проводить структуроване обговорення стратегічних цілей, критичних бізнес-процесів, профілю ризиків та ресурсних можливостей. Результати фіксуються в документі "Організаційний контекст", який служить основою для подальшого визначення цільового стану [31, 43].

Фаза 2: Оцінка поточного стану (As-Is) за NIST CSF 2.0. Організація проходить структуроване опитування за всіма 106 субкатегоріями NIST CSF. Система автоматично присвоює оцінки зрілості 0-5 на основі об'єктивних відповідей. Експертна група валідує результати та за необхідності коригує оцінки. Після завершення оцінки за NIST інструмент через матрицю відповідностей автоматично відображає стан відповідності контролям ISO 27001, процесам COBIT та контролям CIS [24, 30].

Фаза 3: Визначення цільового стану (To-Be) через COBIT 2019. Експертна група використовує структуру COBIT для визначення пріоритетних цілей управління на основі організаційного контексту. Ці цілі через матрицю відповідностей автоматично транслюються у цільовий профіль зрілості NIST CSF (цільовий профіль). Інструмент також показує, які контролі ISO 27001 та контролі CIS будуть необхідні для досягнення цільового стану [35, 36].

Фаза 4: Gap-аналіз та формування дорожньої карти покращень. Інструмент автоматично порівнює «As-Is» та «To-Be», ідентифікуючи прогалини. Формується дорожня карта з конкретними рекомендаціями у термінах всіх чотирьох фреймворків. Експертна група адаптує цю дорожню карту, враховуючи ресурсні обмеження та пріоритетність бізнес-процесів [27, 31].

Переваги, обмеження та перспективи розвитку інструменту

Основні переваги розробленого інструменту включають: єдину точку входу для оцінки відповідності множинним стандартам; уникнення дублювання зусиль через багатостороннє відображення результатів; гнучкість для організацій різного розміру (від МСО з CIS IG1 до великих підприємств з повним COBIT).

Ключові обмеження інструменту: офіційні маппінги між обраними фреймворками було доопрацьовано авторами для забезпечення більш повного покриття; для повної сертифікації ISO 27001 потрібен додатковий детальний аудит документації; автоматизована оцінка може не врахувати всі нюанси організаційного контексту, тому обов'язкова експертна валідація.

Перспективи розвитку включають: інтеграцію додаткових фреймворків (наприклад, NIST SP 800-53, PCI DSS); розробку бібліотеки типових організаційних профілів для різних галузей; автоматизацію генерації документації для сертифікації ISO 27001 на основі результатів оцінки; інтеграцію з GRC-платформами для безперервного моніторингу відповідності.

Таким чином, результатом дослідження є практичний інструмент багатостандартної оцінки кіберзрілості, який поєднує переваги чотирьох провідних міжнародних фреймворків через напівавтоматизований підхід «Human-in-the-Loop». Інструмент забезпечує організаціям можливість отримати комплексний огляд стану кібербезпеки, визначити реалістичний цільовий профіль та сформувати практичну дорожню карту покращень, адаптовану до їхніх специфічних потреб та можливостей.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У сучасному ландшафті кіберзагроз організації все частіше стикаються з необхідністю одночасної відповідності множинним міжнародним стандартам кібербезпеки — NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8 — через регуляторні зобов'язання, вимоги клієнтів та внутрішні політики управління ризиками. Проведення окремих оцінок за кожним стандартом призводить до фрагментації зусиль, дублювання робіт та неефективного використання обмежених ресурсів, особливо критичного для малих та середніх організацій [44-46].

Результатом проведеного дослідження є розробка напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості, який дозволяє організаціям через єдину точку входу — структуроване опитування за базовим фреймворком NIST CSF 2.0 — автоматично отримати оцінку відповідності всім чотирьом провідним міжнародним стандартам без дублювання зусиль. Інструмент виступає як інтелектуальний асистент для експертної групи організації, допомагаючи їй орієнтуватися в складному ландшафті множинних вимог, встановлювати відповідності між різними стандартами та приймати обґрунтовані рішення щодо визначення значущості покращень навіть за умов обмежених ресурсів і часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IBM Security. (2025). Cost of a Data Breach Report 2025. IBM Corporation.
2. Morgan, S. (2025). Cybercrime To Cost The World $12.2 Trillion Annually By 2031. Cybersecurity Ventures. https://cybersecurityventures.com/official-cybercrime-report-2025/
3. NinjaOne. (2025). 7 SMB Cybersecurity Statistics for 2025. https://www.ninjaone.com/blog/smb-cybersecurity-statistics/
4. UK Government. (2025). Cyber Security Breaches Survey 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
5. BD Emerson. (2024). Must-Know Small Business Cybersecurity Statistics for 2025. https://www.bdemerson.com/article/small-business-cybersecurity-statistics
6. Legit Security. (2025). Top IT Security Frameworks. https://www.legitsecurity.com/aspm-knowledge-base/top-it-security-frameworks
7. Dawgen Global. (2023). Beyond NIST: Integrating Multiple Frameworks for Robust Cybersecurity Audits. https://www.dawgen.global/beyond-nist-integrating-multiple-frameworks-for-robust-cybersecurity-audits/
8. Asokan, V. (2025). Comparative Analysis of Cybersecurity Frameworks: NIST, ISO 27001:2022, SOC 2, & COBIT. LinkedIn. https://www.linkedin.com/pulse/comparative-analysis-cybersecurity-frameworks-nist-iso-vikram-asokan-zeznf
9. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
10. International Journal of Advanced Computer Science and Applications. (2025). Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats, vol. 16(6). http://thesai.org/Publications/ViewPaper?Volume=16&Issue=6&Code=ijacsa&SerialNo=72
11. Center for Internet Security. (2024). CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1
12. Center for Internet Security. (2021). CIS Controls Implementation Groups. https://www.cisecurity.org/controls/implementation-groups
13. Cloud Security Alliance. (2024). NIST CSF vs Other Cybersecurity Frameworks. https://cloudsecurityalliance.org/articles/nist-csf-vs-other-cybersecurity-frameworks
14. Orna. (2024). NIST, ISO, COBIT, ITIL: Which Cyber Framework Rules Them All? https://www.orna.app/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all
15. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. Computers & Security, vol. 143, 103920. https://doi.org/10.1016/j.cose.2024.103920
16. Tetteh, A. K., & Asare, P. (2024). Cybersecurity Needs for SMEs. Issues in Information Systems, vol. 25(3), pages 235-246.
17. Armenia, S., & Centra, A. (2021). A Dynamic Simulation Approach to Support the Evaluation of Cyber Security Investments. Decision Support Systems, vol. 147, 113580. https://doi.org/10.1016/j.dss.2021.113580
18. PwC. (2025). Global Digital Trust Insights 2025. TechInformed. https://techinformed.com/cybersecurity-2025-key-stats/
19. Gjeta, L., & Bashota, A. (2024). Digital Transformation in SMEs: Identifying Cybersecurity Risks and Developing Effective Mitigation Strategies. Global Journal of Engineering and Technology Advances, vol. 19(2), pages 116-125.
20. ENISA (2024). Cybersecurity Maturity Assessment for Small and Medium Enterprises. https://www.enisa.europa.eu/tools/cybersecurity-maturity-assessment-for-small-and-medium-enterprises
21. Van Niekerk, J., & Von Solms, R. (2019). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. African Journal of Information and Communication, vol. 23, pages 21-39. https://www.scielo.org.za/pdf/ajic/v23/02.pdf
22. Ozkan, B. Y., & Spruit, M. (2020). Assessing and improving cybersecurity maturity for SMEs: Standardization aspects. *arXiv preprint arXiv:2007.01751*.
23. Ahmed, M., & Panda, S. (2024). SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv preprint arXiv:2408.16140. https://arxiv.org/pdf/2408.16140.pdf

24. Curtin, M., & Moran, B. (2024). Development of a Cyber Risk Assessment Tool for Irish Small Business Owners. arXiv preprint arXiv:2408.16124. https://arxiv.org/pdf/2408.16124.pdf
25. Шевченко, С., Жданова, Ю., & Кравчук, К. (2021). Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *2*(14), 158–175. https://doi.org/10.28925/2663-4023.2021.14.158175
26. Дзюба, L., & Чмир, О. (2022). Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. *Вісник Львівського державного університету безпеки життєдіяльності*, *26*, 47-54. https://doi.org/https://doi.org/10.32447/20784643.26.2022.06
27. Journal of Strategic Defense and Policy Studies. (2025). A Meta-Analysis of Cybersecurity Framework Integration in GRC Platforms: Evidence from U.S. Enterprise Audits. https://jsdp-journal.org/index.php/jsdp/article/view/10
28. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV: International Journal on Informatics Visualization, vol. 4(4), pages 225-232. https://doi.org/10.30630/joiv.4.4.482
29. Center for Internet Security. (2024). CIS Controls v8.1 Mapping to NIST CSF 2.0. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-nist-csf-2-0
30. Yousaf, A., & Khan, M. (2025). STPA-Cyber: A Semi-Automated Cyber Risk Assessment Framework. Computers & Security, vol. 151, 104024
31. Ontario Cyber Security Expert Panel. (2022). Report to the Minister of Public and Business Service Delivery. https://files.ontario.ca/mpbsd-cyber-security-expert-panel-report-en-2022-09-22.pdf
32. ISACA. (2024). The Three Lines Model in Cybersecurity Governance and Risk Management. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/the-three-lines-model-in-cybersecurity-governance-and-risk-management
33. ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. International Organization for Standardization.
34. Scrut Automation. (2025). ISO 27001:2022 Annex A Controls List. https://www.scrut.io/hub/iso-27001/iso-27001-controls
35. ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. https://www.isaca.org/resources/cobit
36. ISACA. (2020). Using COBIT 2019 to Plan and Execute an Organization's Transformation Strategy. https://www.isaca.org/resources/news-and-trends/industry-news/2020/using-cobit-2019
37. Center for Internet Security. (2024). CIS Controls v8 Guide. https://www.cisecurity.org/controls
38. Center for Internet Security. (2022). CIS Controls v8 Implementation Groups Handout. Arkansas Department of Education. https://dese.ade.arkansas.gov/Files/CIS_Controls_v8_Implementation_Groups_handout
39. Center for Internet Security. (2023). Implementation Guide for Small- and Medium-Sized Enterprises CIS Controls IG1. https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises
40. Cyrisma. (2024). What's New in the CIS Critical Controls Version 8.1? https://www.cyrisma.com/whats-new-in-the-cis-critical-controls-v-8-1/
41. CMMI Institute. (2018). Capability Maturity Model Integration (CMMI) for Development, Version 2.0. https://cmmiinstitute.com/cmmi
42. NIST. (2024). NIST Cybersecurity Framework 2.0 Reference Tool. https://csrc.nist.gov/projects/cybersecurity-framework/filters
43. World Economic Forum. (2021). Cyber Risk Governance. https://www.weforum.org/publications/cyber-risk-governance
44. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
45. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
46. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Svitlana M. Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Oleksii S. Kiia
Student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0003-4105-8081
oskiia.fitm24m@kubg.edu.ua

SEMI-AUTOMATED MULTI-STANDARD CYBER MATURITY ASSESSMENT TOOL BASED ON NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 AND CIS CONTROLS V8

Abstract. In today's cyber threat landscape, no software or hardware tool can fully compensate for the lack of a comprehensive approach to security management, which includes both technological and organizational aspects. Modern organizations are often forced to comply with the requirements of several international standards at the same time (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8) due to regulatory obligations, customer requirements and internal policies, which leads to fragmentation of efforts, duplication of work and inefficient use of limited resources. This article is devoted to the development of a semi-automated multi-standard cyber maturity assessment tool that allows organizations to assess compliance with all four frameworks through a single point of entry — a structured survey using the NIST CSF 2.0 framework as a basic measurement tool, COBIT 2019 as a mechanism for determining the target state through prioritization of business processes, ISO/IEC 27001:2022 as a reference for documented controls, and CIS Controls v8 as additional practical detail for small and medium-sized organizations (SMEs). Based on a systematic analysis of scientific literature and practical cases, the necessity of using a mapping matrix between standards for automatic display of assessment results in terms of all four frameworks simultaneously is substantiated. The architecture of the tool is described and the logic of its operation is detailed: from the formation of an expert group and collection of organizational context to the automated assessment of the current state and generation of recommendations for the target. The scientific novelty of the work is the development of a practical tool that combines methodological approaches, namely: multi-standard assessment of the organization's cyber maturity through a correspondence matrix between NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 and CIS Controls v8, which allows you to avoid duplication of efforts when complying with multiple standards; semi-automation of the assessment using objective structured questionnaires, which increases the reliability and repeatability of the results; validation of the results by an interdisciplinary expert group according to the "Human-in-the-Loop" principle, which ensures that the organizational context is taken into account. The role of the expert group as a validator of automatically generated data and a determiner of organizational priorities is characterized, which allows you to combine the advantages of automation with the flexibility of expert analysis. Particular attention is paid to the cost-effectiveness of the proposed solution through the use of publicly available tools (Microsoft Excel) and the possibility of phased implementation for MSOs through the CIS Controls implementation group system (IG1→IG2→IG3).

The results of the study can be used as a practical tool for organizations of any size: small organizations can start at the basic level (CIS IG1) and gradually build maturity, while large enterprises get a comprehensive overview of compliance with multiple standards through a single assessment model without duplication of effort.

Keywords: cyber maturity; multi-standard assessment; NIST CSF 2.0; ISO/IEC 27001:2022; COBIT 2019; CIS Controls v8; semi-automated assessment; expert group; correspondence matrix; roadmap

REFERENCES

1. IBM Security. (2025). Cost of a Data Breach Report 2025. IBM Corporation. https://www.ibm.com/reports/data-breach
2. Morgan, S. (2025). Cybercrime To Cost The World $12.2 Trillion Annually By 2031. Cybersecurity Ventures. https://cybersecurityventures.com/official-cybercrime-report-2025/
3. NinjaOne. (2025). 7 SMB Cybersecurity Statistics for 2025. https://www.ninjaone.com/blog/smb-cybersecurity-statistics/
4. UK Government. (2025). Cyber Security Breaches Survey 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
5. BD Emerson. (2024). Must-Know Small Business Cybersecurity Statistics for 2025. https://www.bdemerson.com/article/small-business-cybersecurity-statistics
6. Legit Security. (2025). Top IT Security Frameworks. https://www.legitsecurity.com/aspm-knowledge-base/top-it-security-frameworks
7. Dawgen Global. (2023). Beyond NIST: Integrating Multiple Frameworks for Robust Cybersecurity Audits. https://www.dawgen.global/beyond-nist-integrating-multiple-frameworks-for-robust-cybersecurity-audits/
8. Asokan, V. (2025). Comparative Analysis of Cybersecurity Frameworks: NIST, ISO 27001:2022, SOC 2, & COBIT. LinkedIn. https://www.linkedin.com/pulse/comparative-analysis-cybersecurity-frameworks-nist-iso-vikram-asokan-zeznf
9. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
10. International Journal of Advanced Computer Science and Applications. (2025). Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats, vol. 16(6). http://thesai.org/Publications/ViewPaper?Volume=16&Issue=6&Code=ijacsa&SerialNo=72
11. Center for Internet Security. (2024). CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1
12. Center for Internet Security. (2021). CIS Controls Implementation Groups. https://www.cisecurity.org/controls/implementation-groups
13. Cloud Security Alliance. (2024). NIST CSF vs Other Cybersecurity Frameworks. https://cloudsecurityalliance.org/articles/nist-csf-vs-other-cybersecurity-frameworks
14. Orna. (2024). NIST, ISO, COBIT, ITIL: Which Cyber Framework Rules Them All? https://www.orna.app/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all
15. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. Computers & Security, vol. 143, 103920. https://doi.org/10.1016/j.cose.2024.103920
16. Tetteh, A. K., & Asare, P. (2024). Cybersecurity Needs for SMEs. Issues in Information Systems, vol. 25(3), pages 235-246.
17. Armenia, S., & Centra, A. (2021). A Dynamic Simulation Approach to Support the Evaluation of Cyber Security Investments. Decision Support Systems, vol. 147, 113580. https://doi.org/10.1016/j.dss.2021.113580
18. PwC. (2025). Global Digital Trust Insights 2025. TechInformed. https://techinformed.com/cybersecurity-2025-key-stats/
19. Gjeta, L., & Bashota, A. (2024). Digital Transformation in SMEs: Identifying Cybersecurity Risks and Developing Effective Mitigation Strategies. Global Journal of Engineering and Technology Advances, vol. 19(2), pages 116-125.

20. ENISA (2024). Cybersecurity Maturity Assessment for Small and Medium Enterprises. https://www.enisa.europa.eu/tools/cybersecurity-maturity-assessment-for-small-and-medium-enterprises
21. Van Niekerk, J., & Von Solms, R. (2019). Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. African Journal of Information and Communication, vol. 23, pages 21-39. https://www.scielo.org.za/pdf/ajic/v23/02.pdf
22. Ozkan, B. Y., & Spruit, M. (2020). Assessing and improving cybersecurity maturity for SMEs: Standardization aspects. *arXiv preprint arXiv:2007.01751*.
23. Ahmed, M., & Panda, S. (2024). SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv preprint arXiv:2408.16140. https://arxiv.org/pdf/2408.16140.pdf
24. Curtin, M., & Moran, B. (2024). Development of a Cyber Risk Assessment Tool for Irish Small Business Owners. arXiv preprint arXiv:2408.16124. https://arxiv.org/pdf/2408.16124.pdf
25. Shevchenko, S. , Zhdanova Y. , & Kravchuk, K. (2021). Information protection model based on information security risk assessment for small and medium-sized business. *Cybersecurity: Education, Science, Technique*, *2*(14), 158–175. https://doi.org/10.28925/2663-4023.2021.14.158175
26. Dziuba, L., & Chmyr, O. (2022). Assessment of information security risks using methodsof mathematical statistics. *Bulletin of Lviv State University of Life Safety*, *26*, 47-54. https://doi.org/https://doi.org/10.32447/20784643.26.2022.06
27. Journal of Strategic Defense and Policy Studies. (2025). A Meta-Analysis of Cybersecurity Framework Integration in GRC Platforms: Evidence from U.S. Enterprise Audits. https://jsdp-journal.org/index.php/jsdp/article/view/10
28. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV: International Journal on Informatics Visualization, vol. 4(4), pages 225-232. https://doi.org/10.30630/joiv.4.4.482
29. Center for Internet Security. (2024). CIS Controls v8.1 Mapping to NIST CSF 2.0. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-nist-csf-2-0
30. Yousaf, A., & Khan, M. (2025). STPA-Cyber: A Semi-Automated Cyber Risk Assessment Framework. Computers & Security, vol. 151, 104024
31. Ontario Cyber Security Expert Panel. (2022). Report to the Minister of Public and Business Service Delivery. https://files.ontario.ca/mpbsd-cyber-security-expert-panel-report-en-2022-09-22.pdf
32. ISACA. (2024). The Three Lines Model in Cybersecurity Governance and Risk Management. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/the-three-lines-model-in-cybersecurity-governance-and-risk-management
33. ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. International Organization for Standardization.
34. Scrut Automation. (2025). ISO 27001:2022 Annex A Controls List. https://www.scrut.io/hub/iso-27001/iso-27001-controls
35. ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. https://www.isaca.org/resources/cobit
36. ISACA. (2020). Using COBIT 2019 to Plan and Execute an Organization's Transformation Strategy. https://www.isaca.org/resources/news-and-trends/industry-news/2020/using-cobit-2019
37. Center for Internet Security. (2024). CIS Controls v8 Guide. https://www.cisecurity.org/controls
38. Center for Internet Security. (2022). CIS Controls v8 Implementation Groups Handout. Arkansas Department of Education. https://dese.ade.arkansas.gov/Files/CIS_Controls_v8_Implementation_Groups_handout
39. Center for Internet Security. (2023). Implementation Guide for Small- and Medium-Sized Enterprises CIS Controls IG1. https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises
40. Cyrisma. (2024). What's New in the CIS Critical Controls Version 8.1? https://www.cyrisma.com/whats-new-in-the-cis-critical-controls-v-8-1/
41. CMMI Institute. (2018). Capability Maturity Model Integration (CMMI) for Development, Version 2.0. https://cmmiinstitute.com/cmmi
42. NIST. (2024). NIST Cybersecurity Framework 2.0 Reference Tool. https://csrc.nist.gov/projects/cybersecurity-framework/filters
43. World Economic Forum. (2021). Cyber Risk Governance. https://www.weforum.org/publications/cyber-risk-governance/

44. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
45. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
46. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.