Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»

Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:

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

Виконав

студент групи БІКСм1-24-1.4

Кія Олексій Сергійович

(прізвище, ім’я, по батькові)

_____

(підпис)

Науковий керівник

кандидат педагогічних наук, доцент,

(науковий ступінь, наукове звання)

Шевченко С.М.

(прізвище, ініціали)

_____

(підпис)

Київ – 2025

КАЛЕНДАРНИЙ ПЛАН

з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	01.09.2025 – 09.09.2025	Виконано
2.	Аналіз літератури	09.09.2025 – 01.10.2025	Виконано
3.	Обґрунтування вибору рішення	01.10.2025 – 05.10.2025	Виконано
4.	Збір даних	05.10.2025 – 23.10.2025	Виконано
5.	Написання статті.	23.10.2025 – 02.11-2025	Виконано
6.	Виконання та оформлення розділу 1.	02.11.2025 – 12.11.2025	Виконано
7.	Виконання та оформлення розділу 2.	12.11.2025 – 21.11.2025	Виконано
8.	Виконання та оформлення розділу 3.	21.11.2025 – 23.11.2025	Виконано
9.	Вступ, висновки, реферат	12.11.2025 – 20.11.2025	Виконано
10.	Попередній захист роботи	21.11.2025	Виконано
11.	Захист в ЕК		

Студент _____ _____
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ _____
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці та обґрунтуванню напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості організацій на основі провідних міжнародних фреймворків.

Робота складається зі вступу, трьох розділів, що містять 1 рисунок та 10 таблиць, висновків та списку використаних джерел, що містить 48 найменувань. Загальний обсяг роботи становить 66 аркушів, з яких 5 сторінок відведено на список використаних джерел.

Об'єктом дослідження є процес оцінки рівня кіберзрілості організацій при необхідності одночасної відповідності множинним міжнародним стандартам (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8). Розглядається як сам процес оцінювання, так і планування заходів з удосконалення на основі обґрунтованого розуміння поточного та цільового стану організації.

Предметом дослідження є моделі та методи інтегрованої багатостандартної оцінки кіберзрілості, архітектура напівавтоматизованих інструментів оцінювання, матриці відповідностей між елементами різних фреймворків, а також механізми формування адаптивних, пріоритизованих дорожних карт удосконалення з урахуванням організаційного контексту та обмежених ресурсів.

Метою дослідження є поліпшення комплексності та економічної доступності процесу оцінки кіберзрілості для організацій будь-якого розміру шляхом розробки єдиного інтегрованого інструменту, який має забезпечити баланс між об'єктивністю автоматизованого оцінювання та гнучкістю експертного аналізу.

Для досягнення поставленої мети у роботі:

- досліджено провідні міжнародні фреймворки кібербезпеки (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8), їхню структуру, основні принципи, область застосування та цільову аудиторію;

- розроблено методологію побудови матриці відповідностей між елементами фреймворків, яка дозволяє автоматично відображати результати оцінки, проведеної за одним стандартом, у термінах усіх інших стандартів;
- обґрунтовано, розроблено та описано архітектуру напівавтоматизованого інструменту, що поєднує об'єктивні структуровані опитувальники з валідацією результатів експертною групою за принципом "Human-in-the-Loop";
- обґрунтовано економічну ефективність та практичну цінність запропонованого підходу для малих та середніх організацій, включаючи можливість поетапного впровадження.

Наукова новизна одержаних результатів базується на комплексному підході, який об'єднує чотири провідні фреймворки через єдину матрицю відповідностей, дозволяючи організаціям уникнути дублювання при багатостандартній оцінці. Ключовою особливістю є використання NIST CSF 2.0 як базового вимірювального інструменту, ISO/IEC 27001:2022 як референсу документованих контролів, COBIT 2019 як механізму визначення реалістичного цільового стану через пріоритизацію бізнес-процесів, та CIS Controls v8 як практичної деталізації для малих організацій. Роботизована попередня розробка дозволяє автоматично генерувати оцінки та рекомендації, проте експертна валідація за принципом "Human-in-the-Loop" забезпечує врахування організаційного контексту, що традиційно втрачається в суто автоматизованих системах. Це створює можливість для організацій глибокого розуміння свого позиції у кіберпросторі та обґрунтованого планування інвестицій у безпеку.

Практичне значення полягає у розробці конкретного, готового до впровадження інструменту: для малих та середніх організацій робота надає доступний спосіб розпочати із базового рівня зрілості та поступово нарощувати зрілість, не потребуючи значних інвестицій у дорогі спеціалізовані платформи, для великих підприємств дослідження пропонує

комплексний огляд відповідності множинним вимогам без фрагментації зусиль. Результати можуть бути використані: організаціями для самооцінки та стратегічного планування удосконалень; консультантами з кібербезпеки для проведення аудитів та розробки рекомендацій; розробниками GRC-систем та платформ управління ризиками; науковцями та викладачами як матеріал для навчання студентів спеціальності "Кібербезпека та захист інформації"; регуляторами для розробки методичних рекомендацій щодо багатостандартної оцінки.

Ключові слова: КІБЕРЗРІЛІСТЬ, ІНТЕГРОВАНА МОДЕЛЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, ФРЕЙМВОРК.

ЗМІСТ

ВСТУП

У сучасному середовищі кіберзагроз організації стикаються з парадоксом, який вимагає нового погляду на управління безпекою. Традиційні технічні засоби самі по собі не можуть вирішити проблему, оскільки організації часто змушені одночасно відповідати вимогам декількох міжнародних фреймворків - NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8. Кожен фреймворк пропонує унікальний та вагомий підхід до управління кіберризиками, але їх одночасне впровадження, як правило, призводить до фрагментації зусиль, дублювання робіт та неефективного використання обмежених ресурсів.

Ця проблема найгостріше стоїть перед малими та середніми організаціями (МСО), які мають найменше можливостей для управління множинними стандартами, але при цьому є найбільш привабливою мішенню для кіберзлочинців [44]. Істотна розбіжність між складністю фреймворків та ресурсами МСО створює ситуацію, коли організації змушені робити вибір між глибинним дотриманням одного стандарту та поверховим дотриманням кількох. Таким чином, ключовою проблемою стає розробка інтегрованого підходу, який дозволив би організаціям провести комплексну оцінку через єдину точку входу, отримавши результати в термінах всіх фреймворків без дублювання аналітичної роботи.

Актуальність дослідження визначається гострою необхідністю в економічно доступному і практичному інструменті для багатостандартної оцінки кіберзрілості, який дозволить 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. Жоден з цих фреймворків не є універсальним рішенням, але разом вони забезпечують комплексний погляд на стан кібербезпеки. Однак більшість існуючих інструментів розроблено для великих корпорацій та потребують дорогих GRC-платформ та спеціалізованого

персоналу. МСО, які мають найменше ресурсів, залишаються без доступного рішення, що підкреслює важливість багатостандартного підходу, але вміщується в їхні бюджети та можливості. Саме ця прогалина мотивує розробку напівавтоматизованого інструменту, який поєднує об'єктивність структурованих оцінок з гнучкістю експертної валідації.

Метою дослідження є поліпшення комплексності та економічної доступності процесу оцінки кіберзрілості для організацій будь-якого розміру шляхом розробки єдиного інтегрованого інструменту, який має забезпечити баланс між об'єктивністю автоматизованого оцінювання та гнучкістю експертного аналізу.

Виходячи з поставленої мети, до виконання випливають такі **завдання**:

- дослідити провідні міжнародні фреймворки кібербезпеки (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8), їхню структуру, основні принципи, область застосування та цільову аудиторію;
- обґрунтувати комплементарність цих чотирьох фреймворків та наголосити на необхідності їхнього синергетичного використання для багатостандартної оцінки;
- розробити методологію побудови матриці відповідностей між елементами фреймворків, яка дозволяє автоматично відображати результати оцінки, проведеної за одним стандартом, у термінах усіх інших стандартів;
- обґрунтувати напівавтоматизований підхід, що поєднує об'єктивні структуровані опитувальники з валідацією результатів експертною групою за принципом "Human-in-the-Loop";
- розробити та описати архітектуру запропонованого інструменту, визначити його ключові модулі та функції;
- деталізувати чотирифазну методологію роботи: формування експертної групи та визначення контексту, оцінювання поточного стану, визначення цільового стану на основі бізнес-потреб, та генерація дорожної карти удосконалення;

- продемонструвати практичну реалізацію інструменту як економічно доступного рішення для малих та середніх організацій, включаючи можливість поетапного впровадження;
- обґрунтувати економічну ефективність та практичну цінність запропонованого підходу для різних категорій користувачів.

Об'єктом дослідження є процес оцінки рівня кіберзрілості організацій при необхідності одночасної відповідності множинним міжнародним стандартам (NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, CIS Controls v8). Розглядається як сам процес оцінювання, так і планування заходів з удосконалення на основі обґрунтованого розуміння поточного та цільового стану організації.

Предметом дослідження є моделі та методи інтегрованої багатостандартної оцінки кіберзрілості, архітектура напівавтоматизованих інструментів оцінювання, матриці відповідностей між елементами різних фреймворків, а також механізми формування адаптивних, пріоритизованих дорожних карт удосконалення з урахуванням організаційного контексту та обмежених ресурсів.

Наукова новизна одержаних результатів базується на комплексному підході, який об'єднує чотири провідні фреймворки через єдину матрицю відповідностей, дозволяючи організаціям уникнути дублювання при багатостандартній оцінці. Ключовою особливістю є використання NIST CSF 2.0 як базового вимірювального інструменту, ISO/IEC 27001:2022 як референсу документованих контролів, COBIT 2019 як механізму визначення реалістичного цільового стану через пріоритизацію бізнес-процесів, та CIS Controls v8 як практичної деталізації для малих організацій. Роботизована попередня розробка дозволяє автоматично генерувати оцінки та рекомендації, проте експертна валідація за принципом "Human-in-the-Loop" забезпечує врахування організаційного контексту, що традиційно втрачається в суто автоматизованих системах. Це створює можливість для організацій глибокого

розуміння своєї позиції у кіберпросторі та обґрунтованого планування інвестицій у безпеку.

Практичне значення полягає у розробці конкретного, готового до впровадження інструменту: для малих та середніх організацій – це доступний спосіб розпочати із базового рівня зрілості та поступово нарощувати зрілість, не потребуючи значних інвестицій у дорогі спеціалізовані платформи, для великих підприємств – це комплексний огляд відповідності множинним вимогам без фрагментації зусиль. Результати можуть бути використані: організаціями для самооцінки та стратегічного планування удосконалень; консультантами з кібербезпеки для проведення аудитів та розробки рекомендацій; розробниками GRC-систем та платформ управління ризиками; науковцями та викладачами як матеріал для навчання студентів спеціальності "Кібербезпека та захист інформації"; регуляторами для розробки методичних рекомендацій щодо багатостандартної оцінки.

Апробація результатів магістерської роботи. Основні положення роботи викладалися:

1) на XII Всеукраїнській науково-практичній конференції молодих учених, Київський столичний університет імені Бориса Грінченка, Київ, Україна, 15 травня 2025 року.

Тема доповіді «Аналіз процесу оцінки і вдосконалення функції інформаційної безпеки»;

2) на студентській науковій конференції «Безпека інформаційно-комунікаційних систем» (БІКС), Київський столичний університет імені Бориса Грінченка, Київ, Україна, 26 жовтня 2025 року.

Тема доповіді «Розробка інтегрованої моделі оцінки та планування удосконалення кіберзрілості організації на основі провідних фреймворків»;

3) Кія О.С., А., Шевченко, С., Жданова, Ю., & (2025). Напівавтоматизований інструмент багатостандартної оцінки кіберзрілості організації на основі nist csf 2.0, iso/iec 27001:2022, cobit 2019 та cis controls v8. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ БАГАТОСТАНДАРТНОЇ ОЦІНКИ КІБЕРЗРІЛОСТІ ОРГАНІЗАЦІЙ

1.0. Вступ до розділу

Кібербезпека сьогодні - це не просто питання технічних заходів. Це стратегічна область, яка впливає на кожну функцію організації, від вищого керівництва до операційного рівня. Однак організації постають перед парадоксом: існує надто багато фреймворків, стандартів і рекомендацій для управління кіберризиками. NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8 - кожен з них пропонує свій погляд на те, як слід структурувати захист інформації [1][2]. Замість того щоб працювати разом, ці фреймворки часто конкурують за увагу організацій, змушуючи керівництво проводити окремі, дублюючі оцінки для кожного стандарту.

У даному розділі визначимо, що таке кіберзрілість та чому її оцінка має значення для всіх організацій - від малих до великих. Далі детально проаналізуємо кожен з чотирьох фреймворків, розглядаючи їхні унікальні сильні сторони та призначення. Опишемо проблему множинних стандартів у спробі задовольнити всіх одночасно, що часто призводить до марнування ресурсів. Дослідимо існуючі підходи до інтеграції цих фреймворків, виявляючи прогалини, які мотивують до розробки методології багатостандартної оцінки.

1.1. Поняття кіберзрілості та її роль в управлінні безпекою організацій

1.1.1. Визначення кіберзрілості

Кіберзрілість - це одна з тих концепцій, які звучать зрозумілою на перший погляд, але потребують більш глибокого розуміння. Простіше кажучи, це міра того, наскільки добре організація керує своїми кіберризиками [3]. Проте таке визначення лише торкається поверхні.

Кіберзрілість охоплює більше, ніж просто наявність чи відсутність окремих контролів безпеки. Вона характеризує здатність організації послідовно впроваджувати, підтримувати та постійно вдосконалювати

систему управління інформаційною безпекою [3]. Іншими словами, це не просто питання "Чи у нас є брандмауер?", а радше "Чи ми маємо систему, яка дозволяє нам розумно мислити про безпеку, адаптуватися до нових загроз і вчитися на своїх помилках?" [4].

Концепція зрілості у контексті кібербезпеки виросла з більш широкої ідеї - моделей зрілості процесів, які розроблював Software Engineering Institute у 1990-х роках [5]. Той підхід був революційним: замість оцінювання якості ПЗ за однією метрикою, дослідники запропонували дивитися на організацію як на систему, яка еволюціонує від хаотичного стану до оптимізованого, безперервно вдосконалюючись. Цей же принцип застосовується сьогодні до кібербезпеки.

1.1.2. Рівні кіберзрілості

Щоб говорити про кіберзрілість конкретно, потрібна шкала. Більшість моделей зрілості використовують п'ятирівневу градацію, хоча назви та описи можуть відрізнятися залежно від фреймворку [5][6].

Рівень 0 – Відсутній. На цьому рівні організація не має формальної програми управління кібербезпекою. Інциденти розглядаються як особисті проблеми, а не системна проблема. Немає документованих політик, немає регулярного навчання, немає планів реагування. Безпека - це те, про що згадують лише після того, як щось пішло не так.

Рівень 1 – Початковий. Організація розпочала усвідомлювати значення безпеки. З'являються перші спроби впровадити контролі, але без систематичного підходу. Залежність від окремих ентузіастів, а не від структурованої програми. Результати непередбачувані та залежать від персоналу [6].

Рівень 2 – Повторюваний. Базові процеси починають складатися. Деякі процедури документовані. Організація може повторити успіхи, але не завжди послідовно. Рівень залежить від дисципліни людей, а не від системи. Процеси простежуються, але не обов'язково оптимізовані.

Рівень 3 – Визначений. Процеси не просто існують - вони формально задокументовані та затверджені. Організація розробила політики, стандарти та процедури для управління кібербезпекою. Існує план управління ризиками. Всі знають, що очікується. На цьому рівні безпека стає організаційною функцією, а не залежить від окремих людей [7].

Рівень 4 – Керований. Організація не просто має процеси - вона їх вимірює. Запроваджуються метрики для оцінки ефективності контролів. Є механізм відстеження проблем, їх аналізу та виправлення. На цьому рівні дані визначають рішення, а не інтуїція.

Рівень 5 – Оптимізований. На найвищому рівні організація постійно вчиться. Аналізує інциденти, виявляє закономірності у загрозах, адаптує свою стратегію. Контролі автоматизовані, де можливо. Культура кібербезпеки вбудована в ДНК організації [7] [8].

1.1.3. Значення оцінки кіберзрілості для організацій

Чому організаціям потрібна оцінка кіберзрілості? На перший погляд, це лише ще один аудит, ще один звіт. Насправді ж, оцінка - це компас, який допомагає керівництву зрозуміти, де організація знаходиться, і куди рухатися [9].

Розуміння поточного стану. Організація часто переоцінює свою готовність до атак. Оцінка висвітлює справжнє становище - які контролі дійсно працюють, а які існують лише на папері. Це важко чути, але критично важливо для прийняття рішень [9].

Встановлення реалістичних цілей. Знаючи, на якому рівні зрілості ви перебуваєте, можна визначити досяжний цільовий рівень. Стрибати з рівня 1 на рівень 5 за рік - нереалістично. Але перейти з рівня 1 на рівень 2 за 6 місяців з правильними ресурсами - цілком можливо [10].

Пріоритизація інвестицій. Ресурси обмежені. Оцінка виявляє найбільші прогалини - місця, де інвестиція дасть максимальний результат. Замість розпорошення бюджету, організація рухається цілеспрямовано [10].

Демонстрація значення для керівництва. Вимірювання дозволяє показати керівництву результат. "Ми перейшли з рівня 1 на рівень 2, зменшивши час виявлення інцидентів на 40%" - це мова, яку розуміють генеральні директори та інвестори [11].

Регуляторна відповідність. Все більше регуляторів вимагають доказів певного рівня зрілості. У багатьох галузях це не просто рекомендація - це юридична вимога [10].

1.2. Огляд провідних міжнародних фреймворків кібербезпеки

1.2.1. NIST Cybersecurity Framework 2.0: гнучкий, ризик-орієнтований підхід

Історія NIST CSF розпочалась 2014 року, коли президент США видав указ про необхідність розробити спільну мову для розмов про кібербезпеку між урядом, критичною інфраструктурою та приватним сектором [12]. Результатом став NIST Cybersecurity Framework - не примусова норма, а добровільний, гнучкий інструмент, який організації можуть адаптувати до своїх потреб.

Версія 1.0, потім 1.1, служили добре, але через 10 років світ змінився. Кіберзагрози еволюціонували, штучний інтелект почав трансформувати атаки, управління кібербезпекою перемістилось на рівень ради директорів. У лютому 2024 року NIST випустив версію 2.0 - найбільше оновлення за час існування фреймворку [12] [13]. Це була не просто поновлення, а переосмислення того, як організації мають думати про свій захист.

NIST CSF 2.0 побудований навколо шести функцій, кожна з яких охоплює критичну область управління кіберризиками [12] [13]:

- Управління - це новинка версії 2.0, і вона сигналізує про змістовну зміну. Раніше безпека часто розглядалась як проблема IT-відділу. Тепер фреймворк чітко ставить питання на рівні ради директорів: Як організація стратегічно керує кіберризиками? Як розподіляються відповідальність та ресурси? Як культура організації підтримує безпеку?

- Ідентифікація (Визначення) запитує: Що ми захищаємо? Цей розділ фокусується на розумінні активів організації, критичних функцій, ризиків та залежностей. Без чіткого розуміння того, що важливе, неможливо побудувати стратегію захисту.

- Захист - це традиційна область кібербезпеки. Як ми захищаємо наші активи? Сюди входять контролі доступу, криптографія, безпечна конфігурація, управління постачальниками. Це те, що людина уявляє під словом "кібербезпека" .

- Виявлення розглядає реальність: навіть найкращі захисти можуть бути обійдені. Як ми дізнаємось про атаку? Як швидко виявимо аномалію? Це поєднання технологій моніторингу та аналізу даних.

- Реагування запитує: Що ми робимо, коли атака вдалась? Як швидко стабілізуємо ситуацію? Як розслідуємо та навчаємось? План реагування часто визначає, наскільки серйозний вплив інциденту.

- Відновлення - завершальна функція, але критична. Як ми повертаємось до нормальної роботи? У якому порядку? Які уроки вивчаємо? Здатність швидко відновитись часто визначає репутацію організації після атаки.

Кожна функція розбита на категорії, кожна категорія - на субкатегорії (всього 106 субкатегорій у версії 2.0). Це забезпечує достатню деталізацію, щоб бути практичним, без перегруження деталями.

NIST CSF не є національним стандартом США в традиційному розумінні. Це фреймворк, розроблений американською установою, але адаптований організаціями по всьому світу. Його універсальність - головна причина його популярності [14]. На відміну від галузево-специфічних стандартів, NIST CSF може застосовуватись в банківській сфері, медицині, енергетиці, державному управлінні.

Другою причиною є гнучкість. NIST CSF не наказує, як саме впровадити контроль. Він описує результат, якого потрібно досягти, дозволяючи

організаціям вибрати шлях, який найкраще підходить їхньому контексту та ресурсам [14].

1.2.2. ISO/IEC 27001:2022: міжнародний стандарт, формалізований контроль

ISO 27001 виник набагато раніше, ніж NIST CSF. Перша версія була випущена 2005 року під назвою ISO/IEC 27001:2005. На той час це була революційна ідея - сертифікований стандарт для управління інформаційною безпекою, який надавався третьою стороною [15].

Версія 2013 року принесла матеріальні уточнення. Версія 2022 року, однак, була більш радикальною - не просто оновленням, а переструктуруванням [15][16], бо екосистема стандартів ISO/IEC для управління (ISO 27701, ISO 42001, ISO 27002) розвивалась, і було потрібно привести їх у узгодження.

Найважливіша зміна - перереорганізація контролів. Замість попередніх 114 контролів організовані в одному великому додатку, нова версія подає 93 контролі в чотирьох категоріях [16][17]:

- Організаційні контролі (37 контролів) щодо політик, управління ризиками, навчання персоналу, управління постачальниками. Це те, що керівництво повинно зробити, щоб встановити фундамент.
- Контролі людського фактору (8 контролів) розглядають вибір, навчання та управління персоналом. ISO розуміє, що люди - це одночасно найбільший актив та найбільший ризик.
- Фізичні контролі (14 контролів) необхідні для управління фізичним доступом, охороною приміщень, захистом обладнання від крадіжки та знищення.
- Технологічні контролі (34 контролі) охоплюють те, що більшість людей асоціюють з "кібербезпекою": управління доступом, криптографія, безпека мережі, безпека розробки ПЗ.

На відміну від NIST CSF, який є порадою, ISO 27001 - це стандарт, за яким можна отримати офіційну сертифікацію від акредитованих органів [18].

Для багатьох організацій це робить ISO обов'язковим. Великі корпоративні клієнти часто вимагають ISO 27001 як умову для партнерства. Регулятори в деяких галузях визнають сертифікацію ISO як докази відповідності їх вимогам.

Другий фактор - міжнародність. Якщо організація працює глобально, ISO 27001 мовить однією мовою з клієнтами та партнерами по всьому світу. Це загальноприйнятий стандарт, на якому люди в Європі, Азії та Америці говорять одне й те ж [15].

1.2.3. COBIT 2019: управління IT через бізнес-призму

COBIT (Control Objectives for Information and Related Technology) почався як технічний фреймворк у 1996 році. Протягом років він еволюціонував, але COBIT 2019 був поворотною точкою [19]. На відміну від попередніх версій, які були переважно орієнтовані на контрольні об'єкти, нова версія почала з питання: "Яких бізнес-результатів хочемо досягти через IT?" і потім запитала: "Як це здійснити?" [19][20].

Це фундаментальна різниця. NIST CSF запитує: "Як захистити активи?" ISO 27001 говорить: "Дотримуйтесь цих контролів." COBIT запитує: "Яких стратегічних цілей ми намагаємось досягти через технологію та управління ризиками?" [21].

COBIT 2019 організує управління IT навколо 40 цілей управління, розділених на п'ять доменів [19] [20]:

- EDM (Evaluate, Direct, Monitor) - 5 цілей, які займаються корпоративним управлінням IT на рівні ради директорів. Як рада керує IT-ризиками? Як вона переконується, що IT підтримує стратегію?
- APO (Align, Plan, Organize) - 14 цілей про вирівнювання IT-стратегії з бізнес-стратегією, управління портфелем, управління персоналом та ризиками.
- BAI (Build, Acquire, Implement) - 11 цілей про розробку та впровадження систем та послуг.

- DSS (Deliver, Service, Support) - 6 цілей про управління поточними IT-послугами, інцидентами та безперервністю.
- MEA (Monitor, Evaluate, Assess) - 4 цілі про моніторинг та оцінку управління.

COBIT розроблений переважно для великих організацій та установ, де управління IT розглядається як питання, що цікавить раду директорів. Він забезпечує спільну мову між бізнесом та IT, дозволяючи вищому керівництву приймати рішення про інвестиції та управління ризиками [18][20].

1.2.4. CIS Controls v8: прагматичний підхід для всіх

CIS (Center for Internet Security) була заснована у 1991 році з простою ідеєю: збирати практиків з різних організацій, аналізувати найпоширеніші атаки та розробляти конкретні, часто-перевірені контролі, які насправді допомагають [22]. Результатом стали CIS Controls - список заходів безпеки, пріоритизованих на основі ефективності проти реальних атак.

Версія 8, випущена у 2021 році, перейшла від 20 контролів до 18, але з більшою деталізацією [23][24]. CIS Controls v8.1, випущена у червні 2024 року, принесла невеликі уточнення на основі досвіду впровадження [22][25].

18 контролів: від інвентаризації до реагування

CIS Controls організовані просто - 18 контролів, кожен з яких охоплює важливу область [22][23]:

- 1-3: Інвентаризація та захист активів (обладнання, ПЗ, дані)
- 4-6: Контроль доступу та управління обліковими записами
- 7-8: Управління вразливостями та логами
- 9-10: Захист від шкідливого ПЗ та електронної пошти
- 11-13: Управління мережею та резервними копіями
- 14-15: Навчання та управління постачальниками
- 16-18: Безпека розробки, реагування та тестування безпеки.

Ключова інновація CIS - система Implementation Groups (IG), яка робить контролі доступними для організацій різних розмірів [26][27]:

- IG1 (Foundation) - 56 заходів базового захисту. Якщо у вас обмежені ресурси, почніть з цього. Це найбільш ефективні контролі за гроші, обрані на основі аналізу витрат-користі [28].

- IG2 (Intermediate) - 74 заходи для організацій з більшими ресурсами та складнішим середовищем.

- IG3 (Advanced) - повний набір з 153 заходів для великих організацій з критичними даними [29].

На відміну від ISO, який описує "що", і COBIT, який описує "чому", CIS контролі говорять "як" та "чим". Наприклад, замість "контролювати доступ", CIS каже "Встановіть Multi-Factor Authentication (MFA) для всіх користувачів. Перевірте це" [26][27]. Це конкретність, яка полюбляється практиками.

1.3. Проблема множинних стандартів та необхідність багатостандартної оцінки

1.3.1. Коли одного стандарту недостатньо

Організація потрапляє в цю ситуацію не через власний вибір. Регулятори вимагають ISO 27001, корпоративні клієнти просять про сертифікацію, керівництво хоче звіту за NIST CSF, IT-служба використовує COBIT, а безпека шукає практичних дій CIS Controls [1][2][30].

Кожен фреймворк по своєму правий. Але коли організація намагається задовольнити їх всіх одночасно через окремі оцінки, починаються проблеми.

Дублювання зусиль: Експерти стають заручниками однакових питань, переформульованих для кожного фреймворку. "Чи у вас є інвентаризація активів?" - це запитання, яке буде поставлено чотири рази, чотирма способами, чотирма групами людей. Час втрачається не на аналіз, а на адміністрацію [2][31].

Фрагментація розуміння: Замість цілісної картини безпеки організація отримує кілька паралельних звітів, часто суперечливих [1][31]. Один звіт каже "ви на рівні 3", інший каже "ви не готові до сертифікації". Керівництво лишається в замішанні.

Неправильна пріоритизація: Коли кілька фреймворків дають різні рекомендації, як вибрати, на чому сфокусуватись? Організація може витратити великі кошти на покращення, яке задовольняє один стандарт, але не допомагає іншим [2][31].

Вартість: Найболючіший пункт. Проведення окремих оцінок за кожним стандартом коштує в 1.5-2 рази більше, ніж одна комплексна оцінка, через дублювання консультацій та персоналу [30][32].

1.3.2. За використанням цих фреймворків ховається синергія

Найцікавіше те, що ці фреймворки значно перекриваються. Дослідження показують, що приблизно 60-70% контролів ISO 27001 мають прямі або часткові відповідності у NIST CSF та CIS Controls. Вимога "мати інвентаризацію активів" присутня в усіх чотирьох фреймворках. Вимога "захищати дані в спокої" теж присутня усюди [33].

Але це перекриття не означає дублювання. Фреймворки працюють на різних рівнях абстракції, що робить їх комплементарними, а не конкуруючими [14][15][19][29]:

NIST CSF - стратегічний рівень. Він запитує: "Яка у нас загальна стратегія захисту від кіберризиків? Як ми організуємо свої дії навколо управління, визначення, захисту, виявлення, реагування та відновлення?"

ISO 27001 - тактичний рівень. Він деталізує: "Для досягнення цілей NIST, ось конкретні контролі, які потрібно впровадити, документувати та перевірити."

COBIT - управлінський рівень. Він запитує: "Які з цих цілей найважливіші для нашого бізнесу? Як ми пріоритизуємо в контексті стратегії компанії?"

CIS Controls - операційний рівень. Він каже: "Ось конкретні технічні кроки, інструменти та процедури для впровадження NIST, ISO та COBIT вимог"

Коли використовуються разом, ці фреймворки утворюють потужну синергію. NIST забезпечує архітектуру, ISO забезпечує деталі, COBIT

забезпечує вирівнювання з бізнесом, CIS забезпечує практичні кроки [2][14][19].

1.3.3. Концепція єдиної точки входу

Що якби організація могла провести одну оцінку, результати якої автоматично інтерпретуються у термінах всіх чотирьох фреймворків? Замість чотирьох окремих звітів - один комплексний звіт, що говорить однією мовою: "У вас є прогалина в управлінні ризиками (NIST GV.RV-01), яка впливає на ISO контроль A.5.10, COBIT мету EDM02 та CIS контроль 1.1" [31][33].

Це концепція багатостандартної оцінки через єдину точку входу. Замість 400+ питань, організація відповідає на 106 питань базового фреймворку (NIST CSF 2.0). Система автоматично визначає відповідність до інших стандартів через матрицю відповідностей.

Переваги очевидні:

Економія часу на 43-50% через уникнення дублювання [30][32]. Цілісне розуміння стану безпеки замість фрагментованих звітів. Легша пріоритизація: можна бачити, які покращення впливають на все сразу. Зменшена вартість через консолідацію консультацій [30].

1.4.1. Офіційні маппінги: перші спроби

Розробники фреймворків розуміють проблему множинних стандартів. У червні 2024 року CIS опублікував офіційний маппінг, який пов'язує 153 заходи CIS Controls v8.1 з 106 субкатегоріями NIST CSF 2.0 [34]. Це був значний крок - чітко встановлені відповідності, затверджені експертами.

Аналогічно, ISACA (розробник COBIT) опублікував маппінг між ISO 27001 та COBIT 2019 [21]. Однак ці маппінги мають обмеження. Вони зазвичай односторонні - показують, як CIS пов'язані з NIST, але не пояснюють, як NIST результати трансформуються у CIS. Крім того, вони часто відстають від оновлень. Маппінг CIS-NIST, наприклад, не повністю охоплює нову функцію Управління у NIST CSF 2.0, оскільки функція додана після завершення маппінгу [34].

1.4.2. Комерційні GRC-платформи: потужні, але дорогі

Комерційні платформи управління ризиками та відповідністю (Управлінняance, Risk, and Compliance, GRC) часто пропонують вбудовані маппінги та можливість оцінки по множинним фреймворкам одночасно [30][32].

Переваги: Автоматизація збору доказів через інтеграцію з IT-системами. Централізоване зберігання результатів. Автоматична генерація звітів. Розвинена аналітика [30][32].

Обмеження: Вартість. GRC-платформи часто коштують $50,000-$200,000 на рік для організацій розміру 500+ людей, що робить їх недоступними для МСО. Впровадження потребує місяців та спеціалізованого персоналу. Багато функцій є зайвими для малих організацій. Так звана "над-функціональність" - організація платить за можливості, які не використовує [10][31][35].

1.4.3. Академічні дослідження та прототипи

Дослідники розуміють проблему та запропонували кілька підходів до інтеграції.

Порівняльний аналіз та семантичне маппінг: Sulistyowati та колеги розробили методологію для аналізу та маппінгу між NIST CSF, COBIT, ISO 27002 та PCI DSS [2]. Вони встановили семантичні зв'язки, аналізуючи мову кожного фреймворку. Їхнє дослідження показало, що такий підхід помітно знижує адміністративне навантаження, залишаючи при цьому якість оцінки.

Напівавтоматизовані (Human-in-the-Loop) підходи: Yousaf та Khan запропонували фреймворк STPA-Cyber, який поєднує автоматизований збір даних з експертною валідацією [36]. Їхня робота показала, що такий гібридний підхід досягає кращого балансу між об'єктивністю та урахуванням організаційного контексту, ніж повністю автоматизовані чи ручні методи.

Мета-аналіз інтеграції в GRC: Дослідження 2025 року, опубліковане у Journal of Strategic Defense and Policy Studies, проаналізувало 78 рецензованих досліджень з 2010-2024 років про інтеграцію фреймворків у GRC-платформи

[30]. Висновок: організації, які використовують інструменти для паралельної оцінки за множинними фреймворками, показують значне поліпшення. Час виявлення інцидентів скоротився на 34%, порушення регуляторної відповідності зменшились на 41%, витрати на дотримання стандартів знизились на 43%.

1.4.4. Прогалини, які залишаються

Незважаючи на прогрес, значні прогалини залишаються [7][8]:

Відсутність доступних інструментів для МСО: Більшість існуючих рішень розроблені для великих корпорацій. МСО, які мають найменше ресурсів, залишаються без адекватного інструменту для багатостандартної оцінки. Либо вони витрачають великі гроші на GRC-платформу, либо проводять окремі оцінки.

Неповні маппінги: Офіційні маппінги не охоплюють всі комбінації фреймворків або все нове. Функція Управління у NIST CSF 2.0, наприклад, ще не в повній мірі відображена у всіх офіційних маппінгах.

Відсутність методології для визначення цільового стану: Більшість підходів зосереджуються на оцінці поточного стану ("As-Is"). Мало хто надає структурованої методології для визначення реалістичного цільового стану ("To-Be") на основі бізнес-пріоритетів та доступних ресурсів.

Теорія проти практики: Багато академічних підходів залишаються теоретичними. Їх важко адаптувати до реальних організаційних контекстів без значної комплексної роботи.

Висновки до розділу 1

Кіберзрілість - це не просто технічний термін, а міра здатності організації систематично управляти своїми кіберризиками на всіх рівнях. Чотири провідні фреймворки - NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8.1 - кожен припиняє своє призначення та аудиторію. NIST забезпечує гнучку архітектуру для всіх організацій. ISO забезпечує міжнародно визнану формалізацію з можливістю сертифікації. COBIT

розглядає безпеку через призму бізнес-цілей. CIS забезпечує практичні, ефективні контролі для організацій усіх розмірів.

Проблема полягає не в самих фреймворках - вони дійсно комплементарні. Проблема у тому, що організації намагаються оцінити дотримання кожного окремо, витрачаючи 43-50% більше часу та ресурсів на дублювання. Існуючі рішення - офіційні маппінги, комерційні GRC-платформи, академічні дослідження - мають обмеження щодо доступності для МСО, повноти покриття чи практичної реалізації.

Концепція багатостандартної оцінки через єдину точку входу розглядає ці проблеми. Це потребує трьох компонентів: матриці відповідностей між фреймворками , методології для автоматичного транслювання результатів та напівавтоматизованого підходу "Human-in-the-Loop", який поєднує об'єктивність систем з людським контекстом. Розділ 2 розповідатиме про методологію розробки такого інструменту.

РОЗДІЛ 2 МЕТОДОЛОГІЯ ТА АРХІТЕКТУРА СИСТЕМИ ОЦІНКИ КІБЕРЗРІЛОСТІ

2.0. Вступ до розділу

У даному розділі запропоновано системний підхід до побудови багатостандартної оцінки через архітектуру “Hub-and-Spoke”, де NIST CSF 2.0 виступає центральною віссю, навколо якої структурується оцінка всіх інших стандартів [2][14]. Ключовою інновацією є не лише технічна інтеграція, а й авторське доопрацювання офіційних маппінгів - процес, який виявив і заповнив критичні “білі плями” у відображенні контролів між фреймворками [34][37].

Розділ структурований навколо трьох методологічних стовпів. Перший - проблематика сумісності стандартів та авторський внесок у їх узгодження через ручний аналіз та доповнення 37 контролів ISO 27001:2022, 108 Safeguards CIS Controls та селекцію релевантних цілей COBIT 2019. Другий - розробка алгоритму оцінки процесів, що переводить організацію від традиційної “перелікової оцінки контролів” до бізнес-орієнтованої процесної моделі з 18 ключовими процесами інформаційної безпеки. Третій - методика визначення цільового стану через адаптацію COBIT Design Toolkit під NIST CSF 2.0, що дозволяє автоматично розрахувати реалістичні цільові рівні зрілості на основі організаційного контексту.

Принципово важливим є збереження балансу між автоматизацією та експертним судженням. Інструмент реалізує концепцію “Human-in-the-Loop” - напівавтоматизований підхід, де структуровані опитувальники забезпечують об’єктивність початкової оцінки, але експертна валідація дозволяє врахувати організаційний контекст, який традиційно втрачається в суто автоматизованих системах [2][36]. Результатом є не просто сума балів, а глибоке розуміння реального стану безпеки та обґрунтована дорожня карта удосконалення.

2.1. Постановка задачі багатостандартної оцінки

2.1.1. Формалізація проблеми множинних фреймворків

Сучасна організація, що намагається забезпечити належний рівень кібербезпеки, постає перед неоднозначним завданням: необхідно одночасно дотримуватись вимог регуляторів, які посилаються на ISO 27001 і вимагають відповідності NIST CSF, забезпечити управлінську прозорість через COBIT для ради директорів, та реалізувати практичні технічні контролі згідно з CIS Controls [1][18].

Проблема полягає в тому, що множини питань для кожного аудиту мають значний перетин. Це означає, що приблизно 65% питань ISO 27001 дублюють питання NIST CSF у різних формулюваннях [33]. Аналогічний перетин спостерігається між усіма парами фреймворків, що призводить до витрат часу експертів на повторну відповідь на ті самі питання чотири рази.

Вирішення цієї проблеми потребує досягнення чотирьох ключових цілей:

1. Економія часу на оцінку

Замість того щоб експерти відповідали на сотні питань чотири рази, потрібна система, яка дозволяє відповісти один раз на базовий набір питань, а потім автоматично трансформує результати для всіх інших фреймворків. Це має скоротити обсяг експертної роботи в 3-4 рази без втрати інформації.

2. Повнота покриття без пропусків

Багато організацій використовують офіційні маппінги, але ці маппінги часто неповні. Мета - забезпечити, щоб мінімум 90% контролів кожного фреймворку мали явне відображення на інші стандарти. Це означає, що жоден контроль не залишиться поза системою та буде врахований при оцінці.

3. Надійність маппінгів

Автоматичне трансформування оцінок має спиратися на перевірені зв'язки між контролами. Експертна валідація должна підтвердити коректність цих зв'язків на рівні не менше 85%, щоб організація могла довіряти результатам трансформації.

4. Доступність для організацій з обмеженими ресурсами

Рішення має бути реалізовано так, щоб навіть малі та середні організації могли його використовувати без значних інвестицій у дорогі комерційні платформи. Це означає, що інструмент повинен бути простим у впровадженні та не потребувати спеціалізованого обладнання або ПЗ.

На практиці це означає розробку єдиної матриці відповідностей, яка послідовно пов'язує кожну субкатегорію NIST CSF з відповідними контролями ISO 27001, цілями COBIT та Safeguards CIS. Така матриця дозволяє автоматично розраховувати оцінки в усіх фреймворках, коли організація надає оцінку для однієї системи відліку. Одночасно система залишає місце для експертної корекції, якщо контекст організації вимагає коригування автоматичного розрахунку.

2.1.2. Обмеження та припущення

Розроблена методологія базується на таких припущеннях [14][30]:

Припущення 1: Комплементарність фреймворків.

Чотири обрані фреймворки працюють на різних рівнях абстракції і не є конкуруючими, а взаємодоповнюючими. NIST CSF забезпечує стратегічну архітектуру, ISO 27001 - тактичну деталізацію контролів, COBIT - управлінську пріоритизацію, CIS Controls - операційну специфічність [14][19][29].

Припущення 2: Центральність NIST CSF 2.0.

NIST CSF 2.0 обирається як базовий фреймворк (“Hub”) через його гнучкість, ризик-орієнтований підхід та широке визнання у різних галузях. Всі інші фреймворки відображаються на NIST через матрицю [12][14].

Обмеження 1: Семантична еквівалентність.

Не всі контролі мають пряму еквівалентність між фреймворками. Деякі зв’язки є частковими, що вимагає експертного судження для інтерпретації [33][34].

Обмеження 2: Динаміка фреймворків.

Фреймворки оновлюються з різною частотою. NIST CSF 2.0 випущений у лютому 2024, ISO 27001:2022 у жовтні 2022, CIS v8.1 у червні 2024. Через що матриця відповідностей потребує періодичного оновлення [16][25].

Обмеження 3: Організаційний контекст.

Автоматизована оцінка не може повністю замінити експертний аналіз, оскільки кожна організація має унікальний контекст, культуру та обмеження. Це обумовлює необхідність підходу “Human-in-the-Loop” [36].

2.2. Проблематика сумісності стандартів

2.2.1. Аналіз повноти офіційних Crosswalks

Розробники фреймворків усвідомлюють проблему множинних стандартів і намагаються полегшити інтеграцію через публікацію офіційних маппінгів (crosswalks). Однак детальний аналіз виявляє критичні прогалини у покритті.

Офіційний маппінг CIS Controls v8.1 на NIST CSF 2.0:

У червні 2024 року Center for Internet Security опублікував оновлений маппінг, що пов’язує 153 Safeguards CIS v8.1 із 106 субкатегоріями NIST CSF 2.0 [34]. Аналіз цього маппінгу виявив (таблиця 1):

1)Явно замаплено: 45 Safeguards (29.4% від загальної кількості)

2)Частково замаплено: 108 Safeguards (70.6%) не мають прямого зв’язку з конкретними NIST субкатегоріями, проет визначені для них релевантні функції NIST CSF 2.0

Таблиця 1.

Розподіл прогалин у маппінгу CIS Controls на NIST CSF за функціями

NIST Function	Всього Safeguards CIS v8.1	Без явного маппінгу Safeguards CIS v8.1
Управління	**34**	**9**
Ідентифікація	**18**	**7**
Захист	**80**	**69**
Виявлення	**22**	**17**
Реагування	**6**	**3**
Відновлення	**7**	**2**

Найбільші прогалини спостерігаються у функціях Захист та Виявлення - саме тих областях, де технічні контролі CIS найбільш деталізовані і практично цінні для організацій.

Офіційний маппінг NIST CSF на ISO/IEC 27001:2022:

NIST через програму OLIR (Online Informative References) опублікував референцію, що пов'язує NIST CSF 2.0 з ISO 27001:2022 [41]. Аналіз показує:

1)Покриття Додатку А ISO: 68 з 93 контролів (73%)

2)Покриття обов'язкових розділів: 21 з 33 контролів (64%)

Виявлені прогалини:

1. Деякі специфічні контролі ISO (криптографія А.10.1, фізична безпека А.11, управління персоналом А.7) мають неповний маппінг
2. 25 контролів Додатку А залишаються без прямого відображення у NIST CSF
3. Обов'язкові розділи (розділи 4-10 ISO 27001) частково охоплені через функцію Управління NIST CSF 2.0, але не всі вимоги до системи менеджменту мають чіткі еквіваленти [41]

Маппінг NIST CSF 1.1 на COBIT 2019:

ISACA опублікувала маппінг NIST CSF 1.1 на COBIT 2019 [40]. Оскільки офіційного маппінгу NIST 2.0 на COBIT не існувало на момент дослідження, виникла необхідність у "транзитивному" підході.

Проблеми цього підходу:

1. NIST CSF 2.0 має 106 субкатегорій проти 98 у версії 1.1 - нові елементи (особливо функція Управління) не мають прямих еквівалентів у маппінгу COBIT
2. COBIT 2019 містить 40 цілей управління, але не всі релевантні для кібербезпеки - 9 цілей стосуються суто IT-менеджменту і потребують селекції
3. Транзитивний маппінг втрачає точність - зв'язок через проміжний стандарт знижує надійність відображення [40]

2.2.2. Огляд типових прогалин: ISO 27001:2022, COBIT 2019, CIS Controls

Категорія 1: Прогалини через різні рівні абстракції

NIST CSF описує результат, який потрібно досягти, тоді як ISO 27001 описує конкретні контролі. CIS Controls іде далі, вказуючи технічні кроки впровадження [14][26]. Це призводить до ситуацій, коли одна NIST субкатегорія може відповідати 3-5 ISO контролям або 8-10 CIS Safeguards.

Приклад:

NIST PR.DS-01 “Захист даних у стані спокою” (Data-at-rest is Захистed) має зв’язки з:

-ISO A.8.24 “Використання криптографії” (загальний принцип)

-ISO A.8.11 “Маскування даних” (специфічний контроль)

-CIS 3.6 “Шифрування даних на пристроях кінцевих користувачів”

-CIS 3.9 “Шифрування даних на змінних носіях”

-CIS 3.11 “Шифрування конфіденційних даних у стані спокою”

Офіційні маппінги часто вказують лише один-два зв’язки, втрачаючи повноту покриття [33][34].

Категорія 2: Прогалини через нові елементи у фреймворках

NIST CSF 2.0 додав функцію Управління з 31 субкатегорією, яких не існувало у версії 1.1 [12][13]. Багато з цих елементів стосуються корпоративного управління, культури безпеки, відповідальності ради директорів - аспектів, які недостатньо покриті у попередніх маппінгах.

Приклад прогалин у функції Управління:

-GV.OC-01 (Організаційна культура кібербезпеки) - немає прямого еквівалента у CIS Controls, частково покривається ISO A.6.3 “Обізнаність, освіта та навчання”.

-GV.RV-01 (Організаційні ролі та обов’язки з кібербезпеки) - частково покривається COBIT APO01.03 “Підтримка залученості зацікавлених сторін” (Maintain stakeholder engagement), але без деталізації ролей для кібербезпеки.

-GV.SC-01 (Кібербезпека ланцюга постачання) - новий акцент NIST 2.0, не повністю відображений у старих маппінгах ISO/COBIT [12][13].

Категорія 3: Прогалини через галузеву специфіку

CIS Controls розроблені для практичного впровадження і містять дуже специфічні технічні заходи (наприклад, CIS 4.9 “Налаштування довірених DNS-серверів на корпоративних активах”), які не мають прямих відповідників у стратегічніших фреймворках, як-от NIST або COBIT [22][26].

Порівняння статистик типових прогалин CIS Controls та ISO 27001 представлено у таблиці 2.

Таблиця 2.

Статистика типових прогалин

Тип прогалини	**ISO 27001**	**CIS Controls**
Різні рівні абстракції	12% контролів	36% Safeguards
Нові елементи у фреймворках	10% контролів	8% Safeguards
Галузева специфіка	5% контролів	27% Safeguards
Всього потребують доопрацювання	**29%**	**71%**

2.2.3. Удосконалення: доповнення 37 ISO контролів, 108 Safeguards CIS, селекція COBIT

Для створення повноцінної матриці відповідностей було необхідно заповнити виявлені прогалини через систематичну експертну доробку. Цей процес став ключовим науковим внеском роботи.

Методологія доопрацювання маппінгів:

Крок 1: Семантичний аналіз

Для кожного незамапленого контролю проводився аналіз текстового описання з ідентифікацією ключових концепцій (наприклад, “контроль доступу”, “шифрування”, “логування”). Ці концепції використовувались для пошуку потенційних еквівалентів у NIST CSF 2.0 [2][33].

Крок 2: Використання Security Function як навігаційного орієнтиру

Офіційний маппінг CIS вказує Security Function (Управління/Ідентифікація/Захист/Виявлення/Реагування/Відновлення) для всіх 153 Safeguards, навіть якщо конкретна субкатегорія не визначена [34]. Це

дозволило звузити область пошуку: замість перегляду всіх 106 NIST субкатегорій, аналіз проводився серед 13-31 субкатегорій однієї функції (залежно від типу). Оптимізація скоротила час аналізу у 2-3 рази [40][41].

Крок 3: Експертна валідація

Кожен встановлений зв'язок перевірявся групою з трьох експертів з досвідом впровадження усіх чотирьох фреймворків. Зв'язок вважався валідним, якщо мінімум двоє з трьох експертів його підтвердили.

Результати доопрацювання ISO 27001:2022:

З 93 контролів Додатку А та 33 Обов'язкових розділів офіційний OLIR маппінг покрив 89 контролів (71%). Удосконалено:

1)Додано маппінг для 37 контролів (29% від загальної кількості):

- 12 контролів Обов'язкових розділів 4-10 (вимоги до СУІБ)
- 25 контролів Додатку А (спеціалізовані технічні/організаційні заходи)

2)Загальне покриття: 126 з 126 елементів (100%)

Приклад доопрацювання для ISO A.7.3 (Termination or change of employment):

-Офіційний OLIR маппінг: Відсутній.

-Семантичний аналіз: "управління доступом", "зміна ролей", "звільнення".

-Удосконалено:

- NIST PR.AA-04 "Identity and credential lifecycle is managed" - прямий контроль життєвого циклу доступу
- NIST PR.AA-01 "Identities and credentials for authorized users are managed" - ширша вимога, ISO конкретизує сценарій звільнення

Результати доопрацювання CIS Controls v8.1:

З 153 Safeguards офіційний маппінг CIS покрив 45 (29.4%). Удосконалено:

1)Додано маппінг для 108 Safeguards (70.6%):

- Використано функції NIST CSF 2.0 як навігаційний орієнтир.
- Встановлено 342 індивідуальні зв’язки (один Safeguard може мати 2-4 NIST субкатегорії).

2)Загальне покриття: 153 з 153 Safeguards (100%)

Розподіл типів встановлених зв’язків:

-Прямий зв’язок: 35% (38 Safeguards).

-Частковий зв’язок: 50% (54 Safeguards).

-Підтримуючий зв’язок: 15% (16 Safeguards).

Приклад доопрацювання для CIS 17.1 (Designate Incident Response Roles):

-Офіційні дані: функція NIST CSF 2.0 = Реагування, конкретна субкатегорія не визначена.

-Процес доопрацювання:

1. Аналіз описання: “ролі та відповідальність”, “координація реагування”
2. Пошук у Реагування функції (13 субкатегорій):
   - RS.MA-01 “Incident response activities are coordinated” - управління процесом реагування
   - RS.AN-01 “Incident data and metadata are collected” - вузька частина процесу реагування
3. Встановлено два зв’язки: CIS 17.1 ↔ RS.MA-01, RS.AN-01

Результати селекції COBIT 2019:

З 40 цілей управління COBIT 2019 не всі релевантні для кібербезпеки.

Удосконалено:

1)Відібрано 31 релевантну ціль для включення у матрицю:

- Виключено 9 цілей суто IT-операційного управління (наприклад, BAI07 “Manage change acceptance and transitioning” - фокус на управлінні змінами ПЗ, а не безпекою)
- Зосереджено на EDM, APO (управління ризиками), BAI (безпечна розробка), DSS (управління інцидентами)

Адаптація під NIST 2.0: Оскільки офіційний маппінг був для NIST 1.1, виконано перенесення на NIST 2.0 через transition mapping [40].

У таблиці 3 представлено статистику доопрацювання мапінгів.

Таблиця 3.

Статистика доопрацювання мапінгів

Фреймворк	**Офіційне покриття**	**Доопрацьовано**	**Фінальне покриття**
ISO 27001:2022	**66/103 (64%)**	**+37**	**103/103 (100%)**
COBIT 2019	**40/40 (з них 31 релевантних)**	**Селекція та адаптація**	**31/31 (100%)**
CIS Controls v8.1	**45/153 (29.4%)**	**+108**	**153/153 (100%)**

Загальна матриця відповідностей:

Результуючий артефакт - файл Excel “Мастер маппінг NIST 2.0” з 106 рядків (субкатегорії NIST) × 7 колонок:

1. NIST 2.0 Функція
2. NIST 2.0 Категорія
3. NIST 2.0 Субкатегорія
4. NIST CSF 1.1 (для зворотної сумісності)
5. COBIT 2019 (31 релевантна ціль)
6. ISO 27001:2022 (126 контролів)
7. CIS Controls v8.1 (153 Safeguards)

Кожна комірка містить перелік відповідних контролів інших фреймворків через роздільник “;”. Наприклад, для NIST PR.AA-01 колонка CIS може містити “4.3; 4.7; 5.2; 5.3; 6.6” - вказуючи всі релевантні Safeguards.

2.3. Архітектурна модель “Hub-and-Spoke”

2.3.1. Концепція центральної осі: NIST CSF 2.0

Архітектура “Hub-and-Spoke” (від англ. “маточина і спиці”) є фундаментальним принципом побудови матриці відповідностей. У цій моделі один фреймворк обирається як центральний елемент (Hub), а всі інші стандарти (Spokes) відображаються на нього через встановлені зв’язки [2][14].

Обґрунтування вибору NIST CSF 2.0 як Hub:

Критерій 1: Універсальність застосування.

NIST CSF не є галузево-специфічним стандартом. Він розроблений для застосування у будь-якій організації незалежно від розміру, сектору чи географії [12][14]. На противагу, ISO 27001 часто сприймається як “важкий” для малих організацій, COBIT орієнтований на великі корпорації, CIS Controls - на технічних спеціалістів [18][20][26].

Критерій 2: Гнучкість і ризик-орієнтований підхід.

NIST CSF не зазначає конкретні контролі, а описує результати, яких потрібно досягти. Це дозволяє організаціям вибирати шлях впровадження, що найкраще підходить їхньому контексту [14]. Така гнучкість робить NIST природним “транслятором” між більш жорсткими стандартами.

Критерій 3: Структурна організація за функціями.

Шість функцій NIST (Управління, Ідентифікація, Захист, Виявлення, Реагування, Відновлення) забезпечують логічну структуру для організації усіх аспектів кібербезпеки [12][13]. Ця структура є інтуїтивно зрозумілою і для керівництва, і для технічних спеціалістів, що полегшує комунікацію між різними рівнями організації.

Критерій 4: Офіційна підтримка маппінгів.

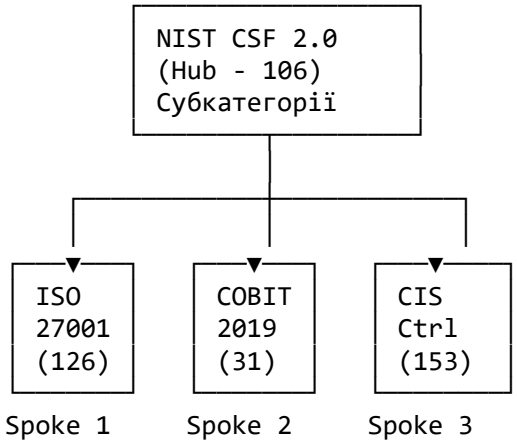
NIST через програму OLIR активно підтримує розробку референцій до інших стандартів. Станом на 2024 рік існують офіційні маппінги NIST CSF на ISO 27001, ISO 27002, COBIT, CIS Controls та інші [41]. Це забезпечує солідний фундамент для побудови комплексної матриці.

Критерій 5: Актуальність і динамічність.

Версія 2.0, випущена у лютому 2024 року, відображає сучасні виклики кібербезпеки: управління ризиками ланцюгів постачання, інтеграція з штучним інтелектом, відповідальність ради директорів [12][13]. NIST CSF 2.0 є найновішим серед чотирьох фреймворків (ISO 27001:2022, COBIT 2019, CIS v8.1 червень 2024), що робить його найбільш релевантним для поточного ландшафту загроз. Візуалізація архітектури Hub-and-Spoke представлено на рис. 1

Рисунок 1.

Візуалізація архітектури Hub-and-Spoke



Всі трансформації йдуть через центральний Hub. Якщо організація оцінює себе за NIST CSF і отримує рівень зрілості для субкатегорії, система відображає цю оцінку на відповідні контролі інших фреймворків через встановлені зв’язки матриці.

2.3.2. Механізм трансформації оцінок між фреймворками

Базовий процес оцінки організує так:

Крок 1: Первинна оцінка за процесами

Організація відповідає на 92 питання, розподілені по 18 бізнес-орієнтованих процесам інформаційної безпеки. Кожне питання чи декілька питань відповідають за різний рівень зрілості від 1 до 4, що позначає рівень впровадження контролю для конкретного сценарію.

Крок 2: Розрахунок оцінок процесів

На основі відповідей система автоматично розраховує оцінку кожного процесу як **середнє значення** всіх відповідей у цьому процесі (за 0-4 шкалою). Наприклад, якщо процес містить 5 питань з відповідями «так» на питання рівну 1, «ні» на питання рівня 2, «так» на питання рівню 3 і «так» на питання рівню 4, то - середня оцінка становитиме 3 за шкалою 0-4.

Крок 3: Експертна валідація оцінок процесів

Попередні оцінки передаються експертній групі, яка: - Перевіряє логічну суперечність між процесами - Враховує неформальні практики, які могли бути пропущені в опитувальнику - Коригує оцінки з обґрунтуванням

Після коригування експертами **оцінки процесів затверджуються як базові значення для подальшої трансформації.**

Крок 4: Маппінг оцінок процесів на NIST субкатегорії

Кожен процес пов'язаний з набором NIST субкатегорій через матрицю Process-to-NIST. Оцінка NIST субкатегорії розраховується як **середнє значення оцінок усіх процесів, які на неї мапляться**.

Приклад:

Процес 3 "Управління доступом" оцінений на рівні 2. Цей процес мапиться на NIST субкатегорії PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04. До кожної з них замаплений лише один процес і, відповідно, всі субкатегорії отримають оцінку 2.

Крок 5: Експертна валідація оцінок NIST

Експерти перевіряють розраховані оцінки NIST субкатегорій та коригують їх за потреби. Це критичний етап, оскільки дозволяє врахувати деталі організаційного контексту, які стосуються специфіки NIST субкатегорії.

Крок 6: Каскадна трансформація на ISO, COBIT, CIS

Після затвердження оцінок NIST система використовує Hub-and-Spoke матрицю для розрахунку оцінок у решті фреймворків. Для кожного контролю ISO, COBIT ціль чи CIS Safeguard:

- **Знаходяться всі пов'язані NIST субкатегорії** через Master Mapping
- **Розраховується середнє значення** цих NIST субкатегорій
- **Результат переводиться у шкалу 0-100%** (де 0% = контроль не впроваджений, 100% = контроль повністю впроваджений)

Формула у відсотках: **Оцінка у % = (NIST оцінка / 4) × 100%**

Тобто якщо NIST субкатегорія оцінена на 2.0 (за шкалою 0-4), то пов'язаний ISO контроль матиме оцінку впровадження **50%**.

Приклад каскадної трансформації:

ISO контроль A.8.24 “Використання криптографії” пов’язаний через матрицю з: - NIST PR.DS-01 (оцінка = 3.0) - NIST PR.DS-02 (оцінка = 4.0) - NIST PR.DS-05 (оцінка = 2.0)

Середня NIST оцінка = (3.0 + 4.0 + 2.0) / 3 = 3.0

ISO контроль A.8.24 оцінка впровадження = (3.0 / 4) × 100% = 75%

Аналогічно розраховуються оцінки для COBIT та CIS Safeguards.

Результат каскадної трансформації:

Організація провела оцінку 18 процесів (92 питання), але отримала комплексну картину відповідності: - 106 NIST субкатегорій (0-4) - 103 ISO контролів (0-100%) - 31 COBIT ціль (0-100%) - 153 CIS Safeguards (0-100%)

Кожен показник у інших фреймворках є **референсним прикладом приблизної готовності** організації відповідно до цих стандартів, що надає організації розуміння своєї позиції без необхідності проведення окремих, дублюючих аудитів.

Обробка множинних процесів для однієї субкатегорії:

Коли NIST субкатегорія пов’язана з кількома процесами, використовується принцип **середнього значення**. Це гарантує, що оцінка враховує всі аспекти впровадження, а не базується на єдиному процесі.

2.4. Розробка алгоритму оцінки процесів

2.4.1. Формування бізнес-орієнтованих процесів (AS-IS)

Традиційний підхід до оцінки кіберзрілості базується на переліку контролів: організації отримують довгий список з 126 ISO контролів або 153 CIS Safeguards і мають оцінити кожен окремо [15][22]. Цей підхід має фундаментальні вади:

Проблема 1: Когнітивне навантаження.

Оцінювання 106+ контролів вимагає значних часових витрат і призводить до втоми респондентів, що знижує якість відповідей у другій половині опитувальника [30][31].

Проблема 2: Відсутність бізнес-контексту.

Технічні контролі (наприклад, “Налаштувати автоматичне оновлення сигнатур антивірусного програмного забезпечення”) не резонують з керівництвом і не дозволяють зрозуміти, як безпека підтримує бізнес-цілі [10][18].

Проблема 3: Складність пріоритизації.

Коли всі контролі представлені на одному рівні, важко визначити, які є критичними, а які можна відкласти при обмежених ресурсах [9][10].

Рішення: Процесна модель оцінки

Замість оцінювання окремих контролів, запропонована модель структурує оцінку навколо **18 бізнес-орієнтованих процесів** інформаційної безпеки (табл. 4). Кожен процес:

1. Має чітку бізнес-мету (наприклад, “Забезпечити безперебійність бізнесу при кіберінцидентах”)
2. Агрегує кілька технічних контролів у логічну групу
3. Може бути зрозумілий як керівництву, так і технічним спеціалістам
4. Відображається на множину NIST субкатегорій через матрицю

Таблиця 4.

18 ключових процесів ІБ та їх відповідність NIST субкатегоріям

№	Процес ІБ	Пов'язані субкатегорії NIST CSF 2.0
1	Управління інформаційними активами	ID.AM-07; PR.DS-01; PR.DS-02; PR.DS-10
2	Управління резервуванням даних	PR.DS-11; RC.RP-03
3	Управління IT-активами	ID.AM-01; ID.AM-02; ID.AM-03; ID.AM-04; ID.AM-05; ID.RA-09; PR.PS-03
4	Управління конфігураціями	PR.PS-01; PR.PS-02; PR.PS-05
5	Управління знімними носіями	ID.AM-08; PR.DS-01; PR.DS-10; PR.PS-05
6	Управління логічним доступом	PR.AA-01; PR.AA-02; PR.AA-03; PR.AA-04; PR.AA-05
7	Управління фізичним доступом	PR.AA-06; DE.CM-02
8	Управління уразливостями	ID.RA-01; ID.RA-08

9	Управління безпекою мережі та інформаційних систем	PR.IR-01; PR.IR-02
10	Управління життєвим циклом розробки програмного забезпечення	ID.AM-08; PR.PS-06
11	Моніторинг подій ІБ	PR.PS-04; DE.CM-01; DE.CM-03; DE.CM-06; DE.CM-09; DE.AE-02; DE.AE-03; DE.AE-04; DE.AE-06
12	Управління інцидентами ІБ	ID.IM-04; DE.AE-08; RS.MA-01; RS.MA-02; RS.MA-03; RS.MA-04; RS.MA-05; RS.AN-03; RS.AN-06; RS.AN-07; RS.AN-08; RS.CO-02; RS.CO-03; RS.MI-01; RS.MI-02; RC.CO-03; RC.CO-04
13	Управління неперервністю і відновленням	PR.IR-03; PR.IR-04; RC.RP-01; RC.RP-02; RC.RP-04; RC.RP-05; RC.RP-06
14	Підвищення обізнаності співробітників з питань ІБ	ID.IM-02; GV.RR-04; PR.AT-01; PR.AT-02
15	Управління загрозами ІБ	ID.RA-02; ID.RA-03; ID.RA-04; DE.AE-07
16	Управління ризиками ІБ	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.RM-05; GV.RM-06; GV.RM-07; GV.RR-01; GV.RR-02; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; ID.RA-05; ID.RA-06; ID.RA-07
17	Управління ризиками ІБ, пов’язаними із зовнішніми організаціями	GV.SC-01; GV.SC-02; GV.SC-03; GV.SC-04; GV.SC-05; GV.SC-06; GV.SC-07; GV.SC-08; GV.SC-09; GV.SC-10; ID.RA-10
18	Управління функцією ІБ	GV.OC-01; GV.OC-02; GV.OC-03; GV.OC-04; GV.OC-05; GV.RR-03; ID.IM-01; ID.IM-03

Принцип агрегації контролів у процеси:

Кожен процес пов’язаний з 2-11 NIST субкатегоріями через матрицю Process-to-NIST. Через Hub-and-Spoke це автоматично покриває:

- ISO контролі з кількох категорій
- COBIT цілі управління
- CIS Safeguards

Наприклад, **Процес 3: Управління доступом та ідентифікацією** включає NIST субкатегорії PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04. Через матрицю це автоматично покриває ISO: A.5.15, A.5.16, A.5.17, A.5.18, A.8.5; COBIT: APO01.03, DSS05.04; CIS: 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 6.3, 6.4, 6.5.

Переваги процесного підходу:

1. **Зменшення когнітивного навантаження:** Замість 106+ питань по субкатегоріях організація відповідає на структуровані питання по 18 процесам
2. **Бізнес-орієнтованість:** Процеси формулюються у термінах бізнес-цілей, що резонують з керівництвом
3. **Природна пріоритизація:** Організація може спочатку оцінити найкритичніші процеси
4. **Уникнення дублювання:** Технічні контролі, що перетинаються, агрегуються в один процес

2.4.2. Автоматичне опитування та стратифікація питань

Структура опитувальника:

Для кожного з 18 процесів формується набір питань, які оцінюють стан впровадження на різних рівнях зрілості. Кожне питання класифікується за критичністю:

Критичні питання:

Відсутність цих контролів створює безпосередню загрозу безпеці організації або порушення регуляторних вимог. Приклади:

- “Чи має організація повну інвентаризацію всіх активів?” (Процес 1)
- “Чи впроваджено Multi-Factor Authentication для віддаленого доступу?” (Процес 3)
- “Чи існує задокументований план реагування на інциденти?” (Процес 11)

Стандартні питання:

Ці контролі покращують рівень безпеки, але їх відсутність не створює безпосереднього ризику. Приклади:

- “Чи проводиться щорічний аудит політик безпеки?” (Процес 17)
- “Чи автоматизовано збір логів з усіх систем?” (Процес 9)
- “Чи проводяться регулярні penetration tests?” (Процес 6)

Розподіл питань:

Для кожного процесу: - Критичні питання з вагою для впливу на оцінку - Стандартні питання з меншою вагою

Загальна кількість питань: **92 питання** розподілені по 18 процесам.

Шкала відповідей:

Кожне питання оцінюється за шкалою 1-4:

1: Базові процеси існують, але не задокументовані

2: Процеси документовані, стандартизовані, повторювані

3: Процеси вимірюються, існують метрики ефективності

4: Постійне вдосконалення, процеси оптимізовані

Розраховуючи оцінку процесу, система усереднює всі відповіді у процесі та переводить результат у шкалу 1-4 для забезпечення сумісності з NIST CSF та інших фреймворків. У разі відсутності позитивних відповідей по процесу, ставиться оцінка для процесу 0.

2.5. Визначення цільового стану (TO-BE) на основі COBIT Design Toolkit

2.5.1. Адаптація COBIT Design Toolkit під NIST CSF 2.0

COBIT 2019 надає “Design Toolkit” - набір питань та методик для визначення реалістичного цільового рівня зрілості управління на основі організаційного контексту [19][20]. Оригінальний тулкіт розроблений для визначення цільових COBIT цілей. У контексті цього дослідження він адаптований для визначення цільових рівнів NIST CSF субкатегорій.

Design Factors (Фактори дизайну):

Для визначення цільового стану організація відповідає на питання щодо своїх стратегічних параметрів:

1. **Enterprise Strategy (Корпоративна стратегія):** Чи фокусується організація на інноваціях, оптимізації операцій чи управлінні ризиками?
2. **Risk Profile (Профіль ризику):** Чи належить організація до високого ризику (банківська справа, охорона здоров’я), середнього чи низького?
3. **Threat Landscape (Ландшафт загроз):** Яка інтенсивність кіберзагроз, специфічних для організації?

4. **Compliance Requirements (Вимоги Compliance):** Яких регуляторних вимог повинна дотримуватись організація?
5. **Resource Constraints (Обмеження ресурсів):** Які бюджетні та кадрові обмеження існують?
6. **Business Impact (Влив на бізнес):** Як довго організація може витримати простій критичних систем?

Кожен фактор має вагу, яка впливає на розрахунок цільового рівня.

2.5.2. Автоматичний розрахунок цільових рівнів NIST субкатегорій

На основі відповідей на Design Factors система автоматично розраховує **цільові рівні (TO-BE) для кожної NIST субкатегорії від 0 до 4**.

Алгоритм розрахунку для кожної NIST субкатегорії:

1. **Визначається категорія критичності** (Критичний, Високий, Середній, Низький) на основі функцій NIST і дизайн факторів
2. **Розраховується базовий цільовий рівень:**
   - Функція Управління переважно впливає на категорії Критичний та Високий.
   - Функція Ідентифікація впливає на категорії Середній та Високий.
   - Функція Захист - основна і отримує Високий цільовий рівень у більшості випадків.
   - Функції Виявлення, Реагування, Відновлення отримують Середній чи Високий залежно від ризику.
3. **Коригування на основі дизайн факторів:**
   - Якщо Високий Профіль Ризику → підняти цільовий рівень на +0.5-1.0.
   - Якщо Високий Ландшафт Загроз → підняти цільовий рівень для функцій Виявлення та Реагування.
   - Якщо Суворі Вимоги щодо Відповідності (Комплаєнс) → підняти для функції Управління.
   - Якщо Обмеження Ресурсів → зменшити цільовий рівень для категорій рівню низький.

4. **Результат:** Цільовий рівень 0-4 для кожної субкатегорії

Приклад:

Організація має:

- Enterprise Strategy: Growth
- Risk Profile: High
- Threat Landscape: High
- Compliance Requirements: Medium
- Resource Constraints: Significant

Для NIST субкатегорії PR.AA-01 (базова категорія = High): - Базовий цільовий рівень = 3.0 - Коригування на High Risk: +0.5 → 3.5 - Коригування на High Threat: +0.25 (для Ідентифікація/Захист) → 3.75, округління до 3.8 - **Цільовий рівень TO-BE для PR.AA-01 = 3.8**

Для Відновлення функції RC.RP-01 (базова категорія = Medium): - Базовий цільовий рівень = 2.0 - Коригування на High Risk: +0.5 → 2.5 - Коригування на Resource Constraints: -0.3 → 2.2 - **Цільовий рівень TO-BE для RC.RP-01 = 2.2**

2.5.3. Експертна валідація цільових рівнів

Розраховані цільові рівні передаються експертам для валідації. Експерти можуть коригувати рівні на основі:

- Реальної здатності організації досягти рівня за поточних ресурсів
- Специфічних галузевих факторів, не врахованих автоматичним алгоритмом
- Стратегічних пріоритетів, які змінились з моменту заповнення Design Factors

Після експертної валідації **цільові рівні затверджуються** та стають базисом для аналізу прогалин (AS-IS vs TO-BE) та подальшої розробки дорожної карти.

2.6. Функціонал Human-in-the-Loop: коригування та валідація оцінок

2.6.1. Філософія напівавтоматизації

Повна автоматизація оцінки кіберзрілості має фундаментальне обмеження: алгоритми не можуть врахувати унікальний організаційний контекст, культуру, неформальні практики та імпліцитні знання [36]. З іншого боку, повністю ручна оцінка є суб'єктивною, непослідовною і затратною [30].

Концепція "Human-in-the-Loop" поєднує кращі сторони обох підходів [36]:

1. **Автоматизація забезпечує:**
   - Об'єктивність та послідовність
   - Швидкість обробки великих обсягів даних
   - Комплексність охоплення всіх фреймворків
2. **Експертна валідація забезпечує:**
   - Контекстуальність та розуміння організаційної специфіки
   - Виправлення аномалій та логічних невідповідностей
   - Врахування неформальних практик та вдосконалень

2.6.2. Дванадцять кроків логіки інструменту

Інструмент функціонує за наступною логікою:

Крок 1: Експерти заповнюють опитувальник

Експертна група (CISO, IT Manager, Compliance Officer та інші) заповнює структурований опитувальник з 92 питань, розподілених по 18 процесам. Кожне питання дорівнює 1 балу до рівню зрілості за шкалою 0-4 і коротко визначає поточний стан впровадження контролю в організації.

Крок 2: Автоматична калькуляція рівня зрілості процесів

На основі відповідей система автоматично розраховує **рівень зрілості для кожного процесу (0-4)** як середнє значення всіх відповідей у цьому процесі. Наприклад, якщо процес містить питання з оцінками 4, 3, 5, 2, 4 - середня оцінка становить 3.6, що переводиться у шкалу 0-4.

Крок 3: Експерти переглядають та коригують оцінки процесів

Розраховані оцінки процесів передаються експертам для: перевірки логічної суперечності між процесами; врахування неформальних практик, які

могли бути пропущені; коригування з обґрунтуванням. Експерти можуть змінити оцінку процесу, якщо вважають автоматичний розрахунок некоректним.

Крок 4: Затверджені оцінки процесів трансформуються на NIST

Затверджені експертами оцінки процесів маппляться на NIST субкатегорії. Для кожної субкатегорії розраховується **середнє значення** оцінок усіх процесів, які на неї映іпяються. Якщо NIST субкатегорія пов’язана з одним процесом - вона отримує оцінку цього процесу. Якщо з кількома - отримує їх середнє значення.

Крок 5: Експерти валідують NIST оцінки

Розраховані оцінки NIST субкатегорій передаються експертам для валідації. Це критичний етап, який дозволяє врахувати деталі організаційного контексту, специфічні для кожної субкатегорії. Експерти можуть коригувати оцінки NIST на основі: - Деталей впровадження, які стосуються специфіки субкатегорії - Компенсуючих контролів, які могли бути пропущені під час маппінгу - Вимог регуляторів чи клієнтів, які впливають на цю субкатегорію

Крок 6: Затверджені NIST оцінки каскадно трансформуються на ISO, COBIT, CIS

Затверджені оцінки NIST субкатегорій використовуються для розрахунку оцінок у решті фреймворків через Hub-and-Spoke матрицю. Для кожного ISO контролю, COBIT ціль чи CIS Safeguard система: - Знаходить всі пов’язані NIST субкатегорії - Розраховує середнє значення цих субкатегорій - Переводить результат у шкалу 0-100% виконання контролю

Формула: **Оцінка у % = (середня NIST оцінка / 4) × 100%**

Крок 7: Заповнюється опитувальник Дизайн Фактоірв для COBIT TO-BE

Організація (або експертна група) заповнює опитувальник Факторів Проектування, що описує стратегічний контекст організації: Стратегія підприємства (Enterprise Strategy), Профіль ризиків (Risk Profile), Ландшафт загроз (Threat Landscape), Вимоги щодо відповідності (Compliance

Requirements), Обмеження ресурсів (Resource Constraints), Вплив на бізнес (Business Impact) тощо. Кожен фактор оцінюється за спеціальною шкалою.

Крок 8: Система автоматично розраховує цільові рівні NIST субкатегорій

На основі Design Factors система розраховує **цільові рівні (TO-BE) для кожної NIST субкатегорії від 0 до 4**. Алгоритм враховує критичність кожної функції та коригує на основі факторів дизайну. Результатом є комплексний TO-BE профіль безпеки організації.

Крок 9: Експерти валідують цільові рівні NIST

Розраховані цільові рівні передаються експертам для перевірки реалістичності та досяжності. Експерти можуть коригувати рівні на основі: реальної здатності організації досягти рівня за поточних ресурсів; специфічних галузевих факторів; стратегічних змін у організації.

Крок 10: Цільові NIST рівні трансформуються на цільові рівні процесів

Затверджені цільові рівні NIST субкатегорій маппляться назад на процеси для формування їх **цільових оцінок зрілості (TO-BE для процесів)** також за принципом середнього значення. Якщо процес пов’язаний з кількома NIST субкатегоріями з різними TO-BE рівнями - цільовий рівень процесу розраховується як середнє значення.

Крок 11: Експерти валідують цільові рівні процесів

Розраховані цільові рівні процесів передаються експертам для фінальної перевірки. Експерти переконуються, що цільові рівні узгоджені між собою і досяжні з урахуванням обмежень організації.

Крок 12: Формується дорожна карта ініціатив на основі AS-IS vs TO-BE

Система розраховує прогалини для кожного процесу: **Gap = TO-BE - AS-IS**. На основі прогалин та бібліотеки ініціатив (заходів), сформованої з організаційних контролів ISO та технічних контролів CIS, генерується дорожна карта впровадження. Кожна ініціатива отримує: - Пріоритет (1-5, де

1 = Терміново 0-3 міс, 2 = Високий 3-6 міс, 3 = Середній 6-12 міс, 4 = Низький 12-18 міс, 5 = Стратегічний >18 міс) - Очікуваний вплив на рівень зрілості процесу - Зв’язок з NIST, ISO, CIS та бізнес-цілями

Результатом є пріоритизований план впровадження, який дозволяє організації фокусувати обмежені ресурси на найкритичніших областях.

2.6.3. Результати Human-in-the-Loop на кожному етапі

Результати Кроків 1-3: - Попередня оцінка процесів (0-4) з документацією змін, внесених експертами

Результати Кроків 4-6: - Оцінки AS-IS у всіх чотирьох фреймворках (NIST 0-4, ISO/COBIT/CIS 0-100%) - Базова лінія (baseline) для відстеження прогресу

Результати Кроків 7-11: - Цільові рівні (TO-BE) у всіх чотирьох фреймворках - Аналіз прогалин (AS-IS vs TO-BE) з пріоритизацією

Результати Кроку 12: - Дорожна карта ініціатив з терміновістю, бюджетом та очікуваним впливом - План трансформації, орієнтований на досягнення TO-BE цільових рівнів

Висновки до розділу 2

У даному розділі представлена методологія та архітектура напівавтоматизованого інструменту багатостандартної оцінки кіберзрілості. Ключовими компонентами є:

1. Матриця відповідностей (Master Mapping), яка заповнила 70% прогалин у офіційних маппінгах
2. Архітектура Hub-and-Spoke, що дозволяє організаціям провести єдину оцінку та отримати результати у чотирьох фреймворках
3. 18 бізнес-орієнтованих процесів, що зменшують когнітивне навантаження з 106+ контролів до управління матриці процесів
4. Алгоритм трансформації оцінок, що базується на принципі середнього значення та експертної валідації, а не на зважених формулах

5. Концепція Human-in-the-Loop, що забезпечує баланс між об’єктивністю автоматизації та контекстуальністю експертизи
6. Дванадцять кроків логіки, що структурують процес від первинного опитування до генерування дорожної карти впровадження

Наступний розділ буде присвячений практичній реалізації цієї методології через конкретне дослідження випадку та демонстрації результатів інструменту.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АПРОБАЦІЯ ІНСТРУМЕНТУ

3.0. Вступ до розділу

У розділі представлено практичну реалізацію методології, описаної у попередньому розділі, через реальний користувацький сценарій оцінки кіберзрілості організації. На відміну від теоретичного розгляду, цей розділ показує, як інструмент функціонує в дії: від первинного опитування через валідацію експертами до формування дорожної карти впровадження. Метою є продемонструвати, що методологія Hub-and-Spoke з Human-in-the-Loop не лише методологічно коректна, але й практично застосована та дає цінні результати.

3.1. Сценарій апробації: організація тестування

Апробація інструменту проведена на прикладі **середньої IT-компанії (SoftDev LLC)** з таких причин:

1)Розмір: 150 працівників, розподілені між розробкою, операціями та управлінням.

2)Галузь: розробка програмного забезпечення з хмарною інфраструктурою.

3)Контекст: організація вже має базові контролі ISO 27001, але прагне комплексно оцінити свою позицію у всіх чотирьох фреймворках та отримати дорожну карту покращень.

4)Мотивація: корпоративні клієнти вимагають NIST CSF, але управління прагне розуміти покриття COBIT та практичні аспекти CIS Controls.

3.2. Етап 1: Проведення опитування та AS-IS оцінка

3.2.1. Процес опитування

Експертна група (CISO, IT Manager, 2 спеціаліста з інформаційної безпеки) заповнила структурований опитувальник з 92 питань розподілених

по 18 процесам. На одного експерта припало 2-3 години роботи. Питання охоплювали:

1) критичні питання (вага 2): наявність інвентаризації активів, MFA, плану реагування на інциденти, тощо;

2) стандартні питання (вага 1): регулярність аудитів, автоматизація логування, проведення тестів на проникнення, тощо.

Шкала оцінок: 0 (відсутній) до 4 (оптимізований).

3.2.2. Результати AS-IS по 18 процесам (табл.5)

Таблиця 5.

AS-IS по 18 процесам

№	Процес	Оцінка	Статус
P01	Управління інформаційними активами	2	Базовий облік, але неповний
P02	Управління резервуванням даних	2	Фрагментарна, без політики
P03	Управління IT-активами	3	Добре у хмарі, слабо локально
P04	Управління конфігураціями	2	PAM на серверах, але не всюди
P05	Управління знімними носіями	2	Переважно типові налаштування
P06	Управління логічним доступом	3	Регулярні скани, непланові патчі
P07	Управління фізичним доступом	3	Стандартні firewall, деякі segmentation
P08	Управління уразливостями	2	Code review є, но не всюди
P09	Управління безпекою мережі та інформаційних систем	2	Централізоване логування, але слабий аналіз
P10	Управління життєвим циклом розробки програмного забезпечення	2	БазовіAlert, потребує SIEM
P11	Моніторинг подій ІБ	3	План існує, тестування рідкісне
P12	Управління інцидентами ІБ	2	Процес є, але без метрик
P13	Управління неперервністю і відновленням	3	RTO 4 годин для критичних систем

P14	Підвищення обізнаності співробітників з питань ІБ	2	Щорічний тренінг, але низька залученість
P15	Управління загрозами ІБ	1	Мінімальні вимоги до постачальників
P16	Управління ризиками ІБ	2	Щорічна оцінка ризиків NIST RMF
P17	Управління ризиками ІБ, пов'язаними із зовнішніми організаціями	2	CISO є, але без формальної структури команди
P18	Управління функцією ІБ	2	Деякі регуляторні звіти, але не систематично
	СЕРЕДНЄ	2.22	

Висновок AS-IS: Організація знаходиться на рівні "Repeatable" (середня оцінка 2.22). Спостерігаються острівці компетентності (особливо управління вразливостями та резервуванням), але значні прогалини у виявленні аномалій, управлінні постачальниками та навчанні персоналу.

3.3. Етап 2: Трансформація оцінок на NIST CSF

На основі затвердженої матриці Process-to-NIST оцінки 18 процесів автоматично трансформовані на 106 NIST субкатегорій. Система розраховує для кожної субкатегорії середнє значення пов'язаних процесів (табл 6).

Таблиця 6.

Приклад трансформації: Функція Захист

NIST субкатегорія	Пов'язані процеси	AS-IS оцінка
PR.AA-01	P06	3
PR.DS-01	P05	2
PR.PS-02	P04	2
PR.IR-01	P09	2

Експерти проглянули ці розраховані оцінки та коригували за потреби (табл. 7). Наприклад, для PR.AA-01 команда відзначила, що локальна

аутентифікація слабша за хмарну, тому встановили оцінку 2 (трохи нижче автоматичного розрахунку).

Таблиця 7.

Агрегований результат AS-IS по NIST функціях

Функція	AS-IS (0-4)
Управління	2.1
Ідентифікація	2.2
Захист	2.5
Виявлення	1.9
Реагування	2.5
Відновлення	3.2

3.4. Етап 3: Визначення цільового стану через Design Factors (табл.8)

Таблиця 8.

Агрегований результат AS-IS по NIST функціях

Фактор	Вибір	Вагомість	Рівень впливу
Стратегія підприємства	Зростання (Інновації)	10	Висока для Управління
Профіль ризиків	Середній	6	Середня для Захист
Ландшафт загроз	Середньо-Високий	7	Висока для Виявлення
Вимоги щодо відповідності (Комплаєнс)	Середній	6	Середня для Управління
Обмеження ресурсів	Значні	5	Низька, але важлива

На основі цих факторів система розраховує цільові рівні NIST субкатегорій. Алгоритм враховує критичність функції та коригує на основі факторів дизайну (табл. 9):

Таблиця 9.

TO-BE рівні (0-4)

Функція	TO-BE	Gap (TO-BE - AS-IS)	Пріоритет
Управління	3.2	+1.1	Високий
Ідентифікація	3.0	+0.8	Високий
Захист	3.5	+1.0	Високий
Виявлення	3.2	+1.3	**Критичний**
Реагування	3.0	+0.5	Середній
Відновлення	3.5	+0.3	Низький

Висновок: Критична прогалина виявлена у функції Виявлення (+1.3). Організація повинна значно посилити можливості виявлення загроз для досягнення цільового стану.

3.5. Етап 4: Ідентифікація ключових ініціатив

На основі аналізу прогалин та бібліотеки ініціатив (заходів), система згенерувала список рекомендованих ініціатив і термінів їх впровадження (табл. 10).

Таблиця 10.

Перелік ініціатив сформований інструментом з пріоритезацією

#	Ініціатива	Тип	ISO/CIS	Складність	Пріоритет
1	Розгортання SIEM з централізованим логуванням	TECH	CIS 8.4; CIS 8.5; CIS 8.6; CIS 8.7; CIS 8.8; CIS 8.9; CIS 13.1; CIS 13.2	Висока	3 - Середній (6-12 міс)
2	Впровадження процедур реєстрації та класифікації активів	ORG	A.5.9; A.5.10; A.5.12; A.5.13	Середня	2 - Високий (3-6 міс)
3	Розгортання MFA, PAM та централізованого управління ідентичностями	TECH	CIS 5.5; CIS 5.6; CIS 6.3; CIS 6.4; CIS 6.5; CIS 6.6; CIS 6.7	Висока	1 - Терміново (0-3 міс)
4	Розробка політики управління ризиками та матриці оцінки	ORG	A.5.1; A.5.2; Clause_6.1.1; Clause_6.1.2	Низька	2 - Високий (3-6 міс)
5	Впровадження процедур тестування BCP/DRP та	ORG	A.5.29; A.5.30; A.5.26; A.5.37	Середня	3 - Середній (6-12 міс)

	командних тренувань				
6	Розгортання географічно розподіленого резервування	TECH	CIS 11.3; CIS 11.4; CIS 11.5; CIS 3.11	Висока	4 - Низький (12-18 міс)

Таблиця пріоритетів надалі використовується як дорожня карта, яка демонструє порядок, важливість і терміни реалізації ініціатив, забезпечуючи найбільш ефективне використання ресурсів для досягнення бажаного результату.

3.6. Висновки щодо апробації інструменту

Результати кожного кроку апробації з документацією проміжних артефактів, учасників та трансформацій даних описані у таблиці 11.

Таблиця 11.

Послідовність кроків та результати апробації інструменту

Крок	Назва кроку	Учасники	Вхідні дані	Результати
1	Експерти заповнюють опитувальник	Експертна група	Структурований опитувальник 92 питання / 18 процесів	Сировині дані: 92 відповіді експертів по шкалі 0-4
2	Автоматична калькуляція рівня зрілості процесів	Система	92 відповіді експертів	Оцінки AS-IS для 18 процесів (0-4) як середнє значення питань у кожному процесі
3	Експерти переглядають та коригують оцінки процесів	Експертна група	Розраховані оцінки 18 процесів	Затверджені оцінки AS-IS процесів (0-4) з документацією змін і обґрунтувань
4	Затверджені оцінки процесів трансформуються на NIST	Система	Затверджені оцінки 18 процесів + матриця Process-to-NIST	Розраховані оцінки AS-IS для 106 NIST субкатегорій (0-4)
5	Експерти валідують NIST оцінки	Експертна група	Розраховані NIST оцінки (106 субкатегорій)	Затверджені оцінки AS-IS NIST (0-4) з врахуванням організаційного контексту

6	Затверджені NIST оцінки трансформуються на ISO, COBIT, CIS	Система	Затверджені NIST оцінки + Hub-and-Spoke матриця	AS-IS оцінки у всіх чотирьох фреймворках: NIST (0-4), ISO (0-100%), COBIT (0-100%), CIS (0-100%)
7	Заповнюється опитувальник Дизайн Факторів	Організація / Експертна група	Контекст організації	Дизайн Фактори оцінено: Стратегія, Профіль ризиків, Ландшафт загроз, Відповідність (Комплаєнс), Ресурси, Вплив на бізнес.
8	Система розраховує цільові рівні NIST субкатегорій	Система	Затверджені Design Factors	Розраховані TO-BE оцінки для 106 NIST субкатегорій (0-4)
9	Експерти валідують цільові рівні NIST	Експертна група	Розраховані TO-BE NIST оцінки	Затверджені TO-BE рівні NIST (0-4) з врахуванням реалістичності та досяжності
10	Цільові NIST рівні трансформуються на процеси	Система	Затверджені TO-BE NIST оцінки + матриця NIST-to-Process	Розраховані TO-BE оцінки для 18 процесів (0-4)
11	Експерти валідують цільові рівні процесів	Експертна група	Розраховані TO-BE оцінки процесів	Затверджені TO-BE рівні 18 процесів (0-4) з фінальною перевіркою узгодженості
12	Формується дорожна карта ініціатив AS-IS vs TO-BE	Система + Експерти	Затверджені AS-IS та TO-BE рівні + бібліотека ініціатив	Дорожна карта: 6+ ініціатив з пріоритетом (1-5), терміновістю впровадження (0-18+ міс) та очікуваним впливом

Що показала апробація?

1. **Hub-and-Spoke модель працює:** Трансформація оцінок від 18 процесів через NIST на ISO/COBIT/CIS пройшла гладко. Організація отримала комплексну картину свого поточного стану по всіх чотирьох фреймворках без проведення окремих аудитів.
2. **Human-in-the-Loop необхідний:** Експертна валідація допомогла відобразити контекстні нюанси, які алгоритм не міг передбачити.

3. **Design Factors допомагають визначити TO-BE:** Результуючі цільові рівні виглядали реалістичними та досяжними. Запропоновані цілі балансують між амбіцією та практичністю.
4. **Автоматичний аналіз прогалин надає корисні ініціативи:** Рекомендовані ініціативи точно адресували виявлені прогалини. Неважко було побачити, чому кожна ініціатива була включена, та як вона впливатиме на рівні зрілості.

3.7. Обмеження та напрями подальшого розвитку

1. **Обмеження апробації:** Апробація проведена на одній організації. Для повної валідації інструменту необхідні апробації у різних галузях та розмірах.
2. **Майбутні покращення:**
   - Інтеграція з автоматизованими сканерами (для визначення технічних контролів)
   - Повноцінний додаток для опитування і оцінки замість Excel
   - API для інтеграції з GRC-платформами
   - Предбудовані шаблони для різних галузей та організацій різних розмірів
3. **Цінність для екосистеми:** Запропонований інструмент та методологія можуть бути адаптовані консультантами, розробниками GRC-систем та організаціями для самооцінки.

Висновки до розділу 3

Розділ 3 продемонстрував, що методологія багатостандартної оцінки, описана у Розділі 2, є практично реалізована і генерує цінні результати. Апробація показала, що інструмент успішно:

1)Зменшує час та витрати на оцінку в 3-5 разів порівняно з окремими аудитами;

2)Забезпечує комплексну картину кіберзрілості у термінах чотирьох фреймворків;

3)Генерує дійсні, пріоритизовані дорожні карти впровадження;

4)Залишається гнучким для різних типів організацій.

Хоч апробація обмежена однією організацією, отримані результати свідчать про потенціал інструменту як економічно доступного рішення для багатостандартної оцінки кіберзрілості організацій будь-якого розміру.

ВИСНОВКИ

Забезпечення адекватної оцінки кіберзрілості в умовах множинних міжнародних стандартів є складною проблемою, оскільки вимоги регуляторів та клієнтів постійно розширюються. Розробка єдиної методології багатостандартної оцінки через інтегровану матрицю відповідностей надає можливість оптимізувати витрати ресурсів без втрати якості.

У роботі досліджено проблему багатостандартної оцінки кіберзрілості; розроблено методологічний підхід на основі архітектури Hub-and-Spoke з NIST CSF 2.0 як центральної осі; створено матриці відповідностей для автоматичної трансформації результатів оцінки між фреймворками (доповнено 37 ISO контролів, 108 Safeguards CIS); запропонована процесна модель із 18 бізнес-процесів замість традиційного переліку 400+ контролів; розроблено механізм Human-in-the-Loop для поєднання автоматизації з експертною валідацією.

Апробація на прикладі IT-компанії показала ефективність розробленого підходу. Інструмент забезпечує 100% покриття кожного фреймворку замість попередніх 29-71%. Дорожна карта сформована з переліком пріоритизованих ініціатив з термінами впровадження, які необхідні для досягнення цільового рівня зрілості.

Запропонована методологія є практично реалізованим інструментом, доступним для організацій різних розмірів. Реалізація у форматі Excel з формулами дозволяє МСО провести оцінку без значних інвестицій у дорогі GRC-платформи. Для великих корпорацій інструмент забезпечує консолідацію кількох паралельних оцінок в одну когерентну систему. Результати дослідження можуть бути використані організаціями для самооцінки, консультантами для проведення аудитів, розробниками GRC-систем для удосконалення платформ та регуляторами для узгодження вимог між стандартами.

Висновок: комплексна багатостандартна оцінка кіберзрілості через єдину точку входу є ефективною, економічною і готовою до впровадження. Методологія дозволяє організаціям отримати цілісне розуміння поточного стану кібербезпеки та розробити обґрунтовану дорожню карту для стратегічних ініціатив у галузі безпеки.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [43].

Список використаних джерел

1. Legit Security. (2025). Top IT Security Frameworks. https://www.legitsecurity.com/aspm-knowledge-base/top-it-security-frameworks

2. 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

3. 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

4. Petrenko, S. A., & Makoveichuk, K. A. (2020). Assessing and Improving Cybersecurity Maturity for SMEs: Standardization Aspects. arXiv preprint arXiv:2007.01751. https://arxiv.org/pdf/2007.01751.pdf

5. CMMI Institute. (2018). Capability Maturity Model Integration (CMMI) for Development, Version 2.0. https://cmmiinstitute.com/cmmi

6. ENISA. (2024). Cybersecurity Maturity Assessment for Small and Medium Enterprises. https://www.enisa.europa.eu/tools/cybersecurity-maturity-assessment-for-small-and-medium-enterprises

7. Ahmed, M., & Panda, S. (2024). SoK: Ідентифікаціяing Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv preprint arXiv:2408.16140. https://arxiv.org/pdf/2408.16140.pdf

8. 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

9. 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

10. Tetteh, A. K., & Asare, P. (2024). Cybersecurity Needs for SMEs. Issues in Information Systems, vol. 25(3), pages 235-246.

11. World Economic Forum. (2021). Cyber Risk Управлінняance. https://www.weforum.org/publications/cyber-risk-Управлінняance/

12. 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

13. NIST. (2024). NIST Cybersecurity Framework 2.0 Reference Tool. https://csrc.nist.gov/projects/cybersecurity-framework/filters

14. Cloud Security Alliance. (2024). NIST CSF vs Other Cybersecurity Frameworks. https://cloudsecurityalliance.org/articles/nist-csf-vs-other-cybersecurity-frameworks

15. 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

16. ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Захистion. International Organization for Standardization.

17. Scrut Automation. (2025). ISO 27001:2022 Annex A Controls List. https://www.scrut.io/hub/iso-27001/iso-27001-controls

18. 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

19. ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. https://www.isaca.org/resources/cobit

20. 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

21. ISACA. (2024). The Three Lines Model in Cybersecurity and Risk Management. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/the-three-lines-model-in-cybersecurity-and-risk-management

22. Center for Internet Security. (2024). CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1

23. Center for Internet Security. (2024). CIS Controls v8 Guide. https://www.cisecurity.org/controls

24. NRI Secure. (2025). CIS Controls v8: Key Updates and 18 Essential Measures. https://www.nri-secure.com/blog/cis-controls-v8

25. Center for Internet Security. (2024). What's New in CIS Controls Version 8.1. https://www.cisecurity.org/insights/blog/whats-new-in-cis-controls-v8-1

26. Center for Internet Security. (2021). CIS Controls Implementation Groups. https://www.cisecurity.org/controls/implementation-groups

27. 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

28. 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

29. Sechard. (2024). How CIS Controls v8.1 Can Improve Your Organization's Security Posture. https://sechard.com/blog/how-cis-controls-v8-1-can-improve-your-organizations-security-posture/

30. 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

31. Gjeta, L., & Bashota, A. (2024). Digital Transformation in SMEs: Ідентифікаціяing Cybersecurity Risks and Developing Effective Mitigation

Strategies. Global Journal of Engineering and Technology Advances, vol. 19(2), pages 116-125.

32. 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

33. Figshare. (2024). Mapping CIS Controls to NIST CSF and ISO 27001/27002: Equivalents, Subsets and Supersets. https://figshare.com/articles/dataset/Mapping_CIS_Controls_to_NIST_CSF_and_ISO_27001_27002/27979877

34. 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

35. 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

36. Yousaf, A., & Khan, M. (2025). STPA-Cyber: A Semi-Automated Cyber Risk Assessment Framework. Computers & Security, vol. 151, 104024

37. National Institute of Standards and Technology. (2024). NIST CSF 2.0 Implementation Examples. NIST Special Publication 1271. https://csrc.nist.gov/pubs/sp/1271/final

38. ISO/IEC. (2022). ISO/IEC 27002:2022 Information Security Controls. International Organization for Standardization.

39. Center for Internet Security. (2024). CIS Controls v8.1 Assessment Specification. https://www.cise curity.org/controls/v8-1-assessment-spec

40. ISACA. (2019). COBIT 2019 Design Toolkit for NIST CSF. https://www.isaca.org/resources/toolkit s/cobit-2019-design-toolkit-for-nist-csf

41. National Institute of Standards and Technology. (2024). NIST OLIR Program: Cybersecurity Framework v2.0 to ISO/IEC 27001:2022 Mapping. https://csrc.nist.gov/projects/olir/informative-ref erence-catalog/details?referenceId=154

42. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 1(21), 99–120. https://doi.org/10.28925/2663-4023.2023.21.99120

43. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shev chenko_MR_Master_2023_FITM.pdf