Vol. 7, No. 2, 2025

DOI: https://doi.org/10.23939/csn2025.02.100

УДК 004.056.5

МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ ВІРТУАЛЬНИХ МЕРЕЖ ТА МОДЕЛІ ЗРІЛОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

О. Ю. Котляров, Л. Л. Бортнік

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: oleksandr.y.kotliarov@lpnu.ua, leonid.l.bortnik@lpnu.ua

Здійснено комплексний аналіз методів оцінки захищеності віртуальних мереж та їх взаємозв'язку з моделями зрілості інформаційної безпеки. Розглянуто ключові технічні підходи – аналіз уразливостей, тестування на проникнення, моделювання загроз та кількісну оцінку ризиків – з урахуванням особливостей мультихмарних і динамічних середовищ. Показано, що поєднання цих методів із процесними моделями (SSE-CMM, NIST Cybersecurity Framework, гібридними підходами на базі ISO/IEC 27001) дає змогу створити багатовимірну систему оцінювання кіберстійкості. Особливу увагу приділено побудові інтегрованих матриць оцінки, які поєднують технічні, організаційні та управлінські метрики (MTTD, MTTR, рівень автоматизації, охоплення patch management).

Дослідження висвітлює практичні сценарії застосування моделей зрілості у великих корпораціях та державних установах, аналізує типові "больові точки" впровадження – технічні (інтеграція у мультихмарних середовищах, сумісність різних рішень), кадрові (дефіцит висококваліфікованих спеціалістів SOC/EDR/SOAR) та економічні (висока вартість платформ і навчання персоналу). Узагальнено сучасні тенденції розвитку, серед яких використання штучного інтелекту й машинного навчання для прогнозування атак, застосування цифрових двійників безпеки як інструменту експериментальної верифікації контролів та інтеграція ESG-стратегій для підвищення корпоративної стійкості.

Отримані результати формують підґрунтя для уніфікованих методик оцінки зрілості та кіберстійкості організацій, забезпечують можливість поєднання технічних і стратегічних вимірів інформаційної безпеки та сприяють переходу від реактивного реагування до проактивного управління ризиками.

Ключові слова: віртуальні мережі, оцінка захищеності, моделі зрілості інформаційної безпеки, кількісна оцінка ризиків, кіберстійкість, штучний інтелект.

Вступ

Сучасна епоха діджиталізації та віртуалізації інформаційних інфраструктур супроводжується не лише експоненційним зростанням обсягів даних та ускладненням бізнес-процесів, а й формуванням якісно нових векторів кіберзагроз. Віртуальні мережі, будучи ключовою основою мультихмарних і контейнеризованих архітектур, стають об'єктами багатовекторних атак, що характеризуються високим ступенем динамічності, адаптивності та здатності до прихованої ескалації. У цих умовах класичні методи захисту, орієнтовані переважно на сигнатурний аналіз і реактивне виявлення загроз, втрачають ефективність, що актуалізує необхідність системного перегляду підходів до забезпечення кіберстійкості організацій.

Попередні дослідження довели, що формування цілісної екосистеми безпеки потребує інтеграції інноваційних рішень – від багатофункціональних NGFW та EDR до оркестраційно-автоматизованих платформ SOAR, здатних синхронізувати дії систем безпеки та зменшувати вплив людського фактора. Водночас залишаються відкритими питання оцінки ефективності цих рішень та визначення рівня зрілості системи інформаційної безпеки (далі – СІБ), що є критично важливим для стратегічного управління ризиками, планування інвестицій та уніфікації з міжнародними стандартами (NIST Cybersecurity Framework, ISO/IEC 27001, SSE-CMM).

Отож постає науково-прикладна проблема інтеграції методів кількісної та якісної оцінки захищеності віртуальних мереж із концепціями зрілості інформаційної безпеки. Її вирішення передбачає формування цілісної методології, здатної забезпечити не лише технічний контроль рівня захисту, а й стратегічне управління кіберризиками, що відповідає вимогам міжнародних стандартів та потребам сучасних організацій у підвищенні своєї кіберстійкості.

Огляд літературних джерел

Проблематика оцінки захищеності віртуальних мереж широко наведена у наукових дослідженнях, де особливу увагу приділено вразливостям віртуалізованих інфраструктур та методам їх кількісного аналізу. Дослідження Bays та ін. [7] детально описують основні загрози для віртуальних мереж, виокремлюючи проблеми мультихмарних середовищ та динамічної сегментації. Подібний підхід демонструє Domínguez-Dorado та співавтори [11], які розглядають засоби виявлення і мінімізації атак у програмно-конфігурованих мережах за допомогою віртуалізованих мережевих функцій.

Систематизація методів оцінки захищеності простежується у праці Tsurkan, Shapoval [19], де акцент зроблено на аналізі ризиків і методиках кількісної оцінки. Wei та співавтори [20] пропонують застосування нейронних мереж для прогнозування атак у комп'ютерних мережах, що відкриває нові перспективи автоматизації процесів оцінювання.

Питання інтеграції методів технічної оцінки з процесними моделями відображено у низці публікацій. Anass та ін. [6] виконали систематичний огляд моделей зрілості інформаційної безпеки, визначивши їх основні сильні та слабкі сторони. Bernardo, Malta, Magalhães [8] розробили оціночну рамку, яка узгоджує оцінку зрілості з NIST Cybersecurity Framework, демонструючи приклад інтеграції технічних та управлінських метрик. В українському науковому просторі питання класифікації та застосування моделей зрілості висвітлили Гребенніков [1] та Худинцев [13], де визначено можливості адаптації міжнародних підходів до національної практики.

Значний масив літератури стосується викликів упровадження зрілісних моделей. Brezavšček та Baggia [9] у своєму систематичному огляді виокремлюють кадрові та економічні обмеження як критичні чинники уповільнення процесу впровадження. Hochstetter-Diez та ін. [12] пропонують методику пріоритизації заходів для державних інституцій, що дає змогу оптимізувати використання ресурсів у контексті обмеженого фінансування.

Сучасні вектори розвитку методів оцінки пов'язуються із використанням штучного інтелекту, цифрових двійників і ESG-орієнтованих стратегій. Acheampong та співавтори [3] досліджують оцінку ризиків із застосуванням VR-середовищ, підкреслюючи роль машинного навчання у виявленні складних атак. Застосування концепції цифрових двійників для імітації сценаріїв атак і перевірки ефективності контролів окреслено у праці Zhou [22], тоді як інтеграція принципів ESG у моделі зрілості стає предметом новітніх досліджень у галузі корпоративної стійкості [9; 12].

Отже, огляд літературних джерел демонструє, що сучасні наукові підходи до оцінки захищеності віртуальних мереж поєднують технічні методи аналізу, процесні моделі зрілості та стратегічні підходи управління ризиками. Водночас ключовими викликами залишаються інтеграція рішень у мультихмарних інфраструктурах, кадровий дефіцит і висока вартість впровадження, що підтверджує актуальність подальших досліджень у цьому напрямі.

Постановка задачі

Аналіз літературних джерел засвідчив, що питання оцінювання захищеності віртуальних мереж у поєднанні з моделями зрілості інформаційної безпеки залишається відкритим та вкрай актуальним. Наявні підходи охоплюють широкий спектр технічних і процесних методик, однак немає уніфікованої системи, яка б давала змогу ефективно інтегрувати результати технічної оцінки з процесними моделями зрілості та забезпечувати комплексне управління кіберризиками. Це зумовлює потребу у створенні нових рішень, що поєднують технічний, організаційний і стратегічний рівні оцінювання.

Мета статті – розробка науково обґрунтованого підходу до оцінювання захищеності віртуальних мереж у контексті моделей зрілості інформаційної безпеки. Для її досягнення передбачається провести узагальнення наукових результатів у сфері систем захисту віртуалізованих середовищ та платформ автоматизованого реагування, зокрема SOAR, SIEM та EDR, розглянувши їх потенціал для формування методологічної основи дослідження. Подальший акцент робиться на систематизації сучасних методів оцінки, серед яких аналіз уразливостей, тестування на проникнення, моделювання загроз і кількісна оцінка ризиків, з урахуванням специфіки мультихмарних і динамічних інфраструктур. Важливим етапом є також класифікація та порівняння наявних моделей зрілості інформаційної безпеки з визначенням їхніх переваг та обмежень у застосуванні для віртуальних мереж.

Особливу увагу приділено створенню інтегрованої методики, яка дасть змогу співвідносити результати технічного аналізу з рівнями зрілості системи інформаційної безпеки та формувати уніфіковані метрики управління ризиками. Дослідження також спрямоване на виявлення ключових викликів впровадження моделей зрілості, серед яких технічні проблеми сумісності, кадровий дефіцит і високі економічні витрати, та пошук шляхів їх подолання. Завершальним завданням є окреслення перспектив розвитку підходів до оцінювання зрілості, які передбачають використання штучного інтеекту для прогнозування атак, застосування цифрових двійників безпеки для експериментальної перевірки ефективності контролів та інтеграцію ESG-орієнтованих стратегій у систему корпоративної стійкості.

Аналітична база дослідження: інтеграція систем захисту та концепції SOAR як основа для оцінки зрілості інформаційної безпеки

Розвиток віртуальних мереж супроводжується впровадженням багаторівневих систем безпеки, до складу яких входять NGFW, IDS/IPS, EDR, SIEM, CASB та рішення для захисту хмарних робочих навантажень (CWPP). Ці технології забезпечують комплексне покриття різних векторів атак, поєднуючи функції превенції, виявлення та реагування. Водночас сам факт наявності розрізнених інструментів не гарантує високого рівня кіберстійкості, оскільки ефективність досягається саме через їх інтеграцію та узгоджене функціонування. Лише комплексний підхід, що охоплює моніторинг, автоматизацію процесів реагування та регулярне оцінювання ефективності, дозволяє забезпечити стійкість до сучасних кіберзагроз.

Актуальним прикладом такої інтеграції є оркестраційно-автоматизовані платформи SOAR, які здатні уніфікувати роботу SIEM, EDR та інших систем безпеки. Вони забезпечують скорочення часу реагування, мінімізацію людського фактора та стандартизацію процесів у межах організації. Саме ці характеристики корелюють із підходами до оцінки зрілості інформаційної безпеки, де одним із ключових показників є рівень автоматизації та керованості процедур.

Отож аналіз сучасних технологій захисту віртуальних мереж та їх інтеграція на базі SOAR створюють концептуальне підґрунтя для подальших досліджень. Вони демонструють перехід від ізольованого застосування окремих рішень до побудови цілісної екосистеми, здатної не лише протидіяти загрозам, а й бути основою для формування формалізованих методів оцінки захищеності та визначення рівня зрілості інформаційної безпеки в організаціях.

Методологічні підходи до оцінки захищеності віртуальних мереж

Оцінювання захищеності віртуальних мереж потребує використання багатовимірних методологічних підходів, які поєднують технічний аналіз, процесну оцінку та ризик-орієнтовані методики. У науковому контексті це дозволяє перейти від локальних перевірок до системного бачення кіберстійкості організації. Кожен метод має власні переваги та обмеження, проте у комплексному застосуванні вони формують основу для інтеграції з моделями зрілості інформаційної безпеки.

Методи аналізу уразливостей (Vulnerability Assessment).

R. Acheampong, D.-M. Popovici та T. C. Balan зазначають, що методи аналізу уразливостей ґрунтуються на систематичному виявленні слабких місць у конфігураціях мережевих сегментів, програмних компонентів і сервісів віртуалізації. Відмінність цього підходу від класичного аудиту полягає у високому рівні автоматизації: застосування сканерів на кшталт Nessus, OpenVAS, QualysGuard дає змогу регулярно перевіряти динамічні інфраструктури та формувати кількісні метрики відповідно до CVSS (Common Vulnerability Scoring System).

У контексті віртуальних мереж цей підхід є особливо релевантним, оскільки системи з динамічним масштабуванням ресурсів (наприклад, Kubernetes чи OpenStack) часто страждають від помилок конфігурацій, неконтрольованого розширення прав доступу, невчасних оновлень віртуальних машин. Аналіз уразливостей дає змогу не лише виявити відомі проблеми, а й зафіксувати системні закономірності, наприклад, повторювані конфігураційні дефекти у середовищах мультихмарної взаємодії. Наукове значення полягає у створенні базису для кількісної оцінки технічного рівня захищеності, який надалі корелює з організаційними процесами у моделях зрілості [3].

Тестування на проникнення (Penetration Testing).

На думку M. M. Khudyntsev, I. L. Palazhchenko, пентест є емпіричною формою оцінювання, що імітує реальні сценарії атак з урахуванням тактик і технік, описаних у MITRE ATT&CK чи OWASP. Його унікальність полягає у тому, що він здатен перевірити експлуатаційну значущість виявлених уразливостей і підтвердити, наскільки легко їх можна використати для реального проникнення.

У віртуальних середовищах пентест охоплює специфічні вектори:

– міжвіртуальні комунікації у межах одного фізичного хоста, де атакувальник може “перестрибнути” з однієї віртуальної машини на іншу;

– мультихмарні взаємодії, які відкривають ризики компрометації через некоректні API-з’єднання та слабкі місця у сервісах федерації ідентичностей;

– гіпервізори та системи оркестрації (наприклад, VMware ESXi, Hyper-V, KVM), де особливо небезпечними є атаки на рівні ескалації привілеїв та втечі з віртуального середовища (VM escape).

Отже, пентест є не лише практичним інструментом, а й методологічним мостом між технічними метриками та реальними сценаріями атак, що робить його невід’ємною складовою оцінки зрілості процесів реагування [13, с. 127].

Методи моделювання загроз (Threat Modeling).

Моделювання загроз є вищим рівнем абстракції, що дає змогу сформувати системне бачення потенційних атак. Воно базується на побудові графів атак, які відображають послідовність кроків зловмисника та вказують на критичні точки компрометації. Найпоширенішими підходами є STRIDE, DREAD та PASTA, що дозволяють оцінювати загрози за категоріями (відмова в обслуговуванні, підробка даних, привласнення ідентичності тощо).

У випадку віртуальних середовищ моделювання загроз набуває додаткової цінності завдяки здатності враховувати:

– політики мікросегментації у віртуальних мережах;

– особливості контейнерних оркестраторів (Kubernetes, Docker Swarm), де атаки можуть поширюватися через загальні реєстри чи некоректні конфігурації pod-ів;

– динамічну змінність топологій, яка вимагає побудови сценаріїв у режимі near real-time.

Отож Threat Modeling не лише структурує можливі сценарії атак, а й створює основу для прогнозного аналізу у межах моделей зрілості, оскільки дає змогу оцінити не лише наявний стан безпеки, а й потенційні траєкторії розвитку загроз [7].

Кількісна оцінка ризиків (Risk Quantification).

Кількісна оцінка ризиків здійснюється відповідно до міжнародних стандартів, зокрема NIST SP 800-30 та ISO / IEC 27005, і полягає у формалізації ризиків через математичні залежності: імовірність реалізації інциденту множиться на масштаб його потенційних наслідків. Це дає змогу перейти від якісного опису до кількісних метрик, що можуть бути інтегровані у системи прийняття управлінських рішень.

У випадку віртуалізованих інфраструктур такі методики мають особливе значення: вони дозволяють поєднувати показники продуктивності й надійності (uptime, SLA, latency) з метриками

інформаційної безпеки (рівень вразливості, імовірність компрометації), утворюючи інтегральні індикатори кіберстійкості. Ключовим аспектом є їхня здатність корелювати з процесними параметрами зрілості, наприклад, часткою автоматизованих процесів реагування чи ефективністю кадрової політики у сфері безпеки.

Отже, кількісна оцінка ризиків забезпечує універсальну мову для комунікації між технічними фахівцями та управлінським рівнем, дозволяючи інтегрувати оцінку кібербезпеки у стратегічне управління організацією.

Узгоджене застосування вказаних методів створює багаторівневу систему оцінки, де:

– аналіз уразливостей і пентест визначають тактичний рівень перевірки;
– моделювання загроз формує стратегічні прогнози розвитку сценаріїв атак;
– кількісна оцінка ризиків забезпечує інтегральний вимір стійкості організації [14].

У комплексі вони формують основу для валідних і масштабованих результатів оцінки, які можуть бути безпосередньо використані у рамках моделей зрілості інформаційної безпеки.

Класифікація моделей зрілості інформаційної безпеки

Розробка та впровадження моделей зрілості інформаційної безпеки є ключовим елементом стратегічного управління кіберризиками, оскільки вони забезпечують не лише формалізацію поточного стану захищеності, а й визначають траєкторії розвитку організаційних процесів. У віртуалізованих середовищах значення цих моделей зростає, адже високий рівень динамічності інфраструктури потребує не тільки тактичних рішень, спрямованих на усунення уразливостей, а й системної оцінки зрілості інформаційної безпеки на процесному, організаційному та стратегічному рівнях.

У сучасній практиці можна виокремити низку моделей, що відрізняються підходами до класифікації зрілості: CMMI-based ISM³, SSE-CMM, NIST Cybersecurity Framework (CSF), а також гібридні системи, побудовані на поєднанні ISO / IEC 27001 та NIST. Їхні основні характеристики наведено у табл. 1.

Таблиця 1

Порівняльна характеристика моделей зрілості інформаційної безпеки

Модель	Методологічна основа	Рівні зрілості	Сильні сторони	Обмеження
CMMI-based ISM³	Модель CMMI, процесний підхід до управління безпекою	Від 1 (початковий) до 5 (оптимізований)	Чітка орієнтація на процеси, інтеграція з корпоративним управлінням	Надмірна формалізація, складність впровадження у малих організаціях
SSE-CMM (ISO / IEC 21827)	Міжнародний стандарт ISO / IEC 21827, орієнтований на системну інженерію	5 рівнів від початкового до оптимізованого	Глибоке охоплення інженерних аспектів, висока деталізація	Вузька фокусованість на технічних процесах, складність інтеграції з бізнес-процесами
NIST CSF	Risk-based framework, категорії: Identify-Protect-Detect-Respond-Recover	4 рівні імплементації (Partial, Risk Informed, Repeatable, Adaptive)	Гнучкість, простота адаптації, сумісність із регуляторними вимогами	Відсутність чіткої градації на процесному рівні, потреба у доповненні ISO 27001
Гібридні моделі (ISO 27001 + NIST)	Інтеграція процесного підходу ISO та risk-based підходу NIST	Від базового до високого рівня інтеграції	Баланс між формалізованим менеджментом і адаптивністю	Методологічна складність, ризик дублювання процедур

Модель CMMI-based ISM³ розвиває класичний підхід Capability Maturity Model Integration у площині інформаційної безпеки. Вона орієнтована на формалізацію процесів та їх поступове вдосконалення, що забезпечує високу керованість, але водночас ускладнює застосування у малих та середніх організаціях через необхідність значних ресурсних витрат [13, с. 128].

SSE-CMM (ISO / IEC 21827) фокусується на інженерних процесах і є цінною для організацій з високим рівнем технологічної складності. Вона забезпечує детальне охоплення технічних аспектів безпеки, проте має обмежену придатність для оцінки управлінських і бізнесових параметрів зрілості.

NIST Cybersecurity Framework (CSF) вирізняється гнучкістю та орієнтацією на управління ризиками. Його п'ять категорій (Identify, Protect, Detect, Respond, Recover) формують основу адаптивної стратегії безпеки, що особливо ефективно у середовищах з високою мінливістю, таких як віртуалізовані мережі. Недоліком є відсутність чіткої градації процесної зрілості, що обмежує його застосування у довгострокових програмах розвитку безпеки.

Нарешті, гібридні моделі, які поєднують ISO / IEC 27001 та NIST CSF, дають змогу досягти балансу між процесним менеджментом і ризик-орієнтованим підходом. A. Brezavšček та A. Baggia відзначають, що гібридні моделі забезпечують синергію формальної сертифікаційної основи ISO та гнучкої адаптивності NIST, однак потребують високої методологічної зрілості для уникнення дублювання процедур та конфлікту між різними стандартами [9].

Тож класифікація моделей зрілості демонструє, що кожна з них має власну нішу застосування: від інженерних рішень у високотехнологічних інфраструктурах до стратегічного управління ризиками у динамічних віртуальних мережах. Це дає змогу сформувати підхід, де вибір моделі визначається не лише технологічними параметрами, а й організаційними характеристиками та цілями розвитку кіберстійкості.

Додатково варто зазначити, що моделі зрілості інформаційної безпеки суттєво відрізняються за підходами до інтеграції з корпоративним управлінням. Наприклад, CMMI-based ISM³ та SSE-CMM акцентують увагу переважно на внутрішніх процесах організації, тоді як NISTCSF та гібридні моделі охоплюють зовнішні фактори, включно з нормативними вимогами та управлінням ризиками постачальницького ланцюга. Це є особливо важливим у сучасних умовах, коли велика частина інфраструктури організацій функціонує у хмарних середовищах, де ризики третіх сторін є критично значущими [17, с. 4–5].

Потрібно виокремити і появу адаптованих варіацій моделей зрілості, розроблених спеціально для секторів критичної інфраструктури, таких як енергетика, транспорт чи охорона здоров'я. У цих галузях моделі на кшталт Cybersecurity Capability Maturity Model (C2м²), яку запропонувало Міністерство енергетики США, демонструють більш прикладний характер та орієнтованість на практичні метрики. Це свідчить про тенденцію переходу від універсальних рамок до галузево-специфічних моделей, які враховують особливості технологічних процесів та вимоги регуляторів.

Дослідники L. Bernardo, S. Malta, J. Magalhães вважають, що важливим напрямом розвитку моделей зрілості є їх інтеграція з кількісними метриками кіберстійкості, такими як середній час виявлення та реагування на інциденти (MTTD, MTTR), відсоток автоматизації процесів реагування чи охоплення patch management. Такі показники створюють міст між технічними перевірками та стратегічними рамками, надаючи організаціям можливість оцінювати прогрес у динаміці. Це особливо актуально для віртуальних мереж, де топології та навантаження змінюються у режимі реального часу [8].

Для підтвердження цього положення було змодельовано приклад інтегрованої матриці оцінювання для умовної організації, яка експлуатує мультихмарну інфраструктуру (табл. 2).

Отримані результати демонструють, що організація досягає середнього рівня зрілості за окремими категоріями, однак має "вузькі місця" у швидкості реагування, покритті критичних оновлень і навчанні персоналу. Інтеграція чисельних показників у процесні моделі зрілості дає змогу не лише оцінити поточний стан системи, а й визначити конкретні напрями інвестування: підвищення рівня автоматизації реагування, скорочення часу застосування патчів, розширення програм підготовки кадрів.

Загальною тенденцією останніх років є включення у моделі зрілості нефінансових і нефункціональних вимірів, зокрема аспектів ESG (Environmental, Social, Governance). Кіберстійкість дедалі частіше трактується не лише як технічний показник безпеки, а як елемент корпоративної

відповідальності та довіри з боку стейкхолдерів. Отож сучасні моделі зрілості інформаційної безпеки еволюціонують у напрямі комплексних рамок управління ризиками, що враховують як технічні, так і соціально-економічні чинники [11].

Таблиця 2

Інтегрована матриця оцінювання захищеності та зрілості СІБ

Показник	Значення	Референсне значення	Інтерпретація рівня зрілості
MTTD (Mean Time to Detect)	14 год	≤ 12 год	Відповідає рівню *Risk Informed* (потрібне скорочення часу виявлення)
MTTR (Mean Time to Respond)	36 год	≤ 24 год	Низький рівень процесної зрілості (*Partial*)
Рівень автоматизації процесів реагування	42 %	≥ 60 %	Перехідний рівень (*Repeatable*), рекомендоване впровадження SOAR
Patch Management Coverage	78 %	≥ 90 %	Середній рівень зрілості (*Risk Informed*), критичні оновлення застосовуються із затримкою
Security Awareness Index	65 %	≥ 80 %	Потребує посилення навчальних програм (*Initial-Repeatable*)

Інтеграція методів оцінки з моделями зрілості

Ефективне управління інформаційною безпекою у віртуалізованих середовищах потребує не лише ізольованого застосування методів технічного тестування чи процесних стандартів, а й їх синхронізації в єдину систему. Саме інтеграція методів оцінки з моделями зрілості дає змогу трансформувати результати технічного аналізу у стратегічно значущі метрики, що відображають загальний рівень кіберстійкості організації.

Дослідник W. Zhou зазначав, що важливо корелювати результати технічних перевірок із рівнями зрілості інформаційної безпеки. Дані аналізу уразливостей та пентестів можна зарахувати до рівнів за моделями CMMI-based ISM³ чи NIST CSF: критичні уразливості на початкових етапах без політик усунення свідчать про низьку зрілість (Initial/Partial), тоді як структуровані процеси управління уразливостями та повторювані пентести відповідають вищим рівням (Managed, Repeatable, Optimized) [22, с. 179].

Другий етап – *побудова інтегрованих матриць оцінки*, де поєднуються технічні, процесні та організаційні показники. Така матриця може охоплювати одночасно результати VA/пентестів, наявність стандартизованих процедур реагування (наприклад, за NIST CSF) та кадрові параметри (наявність SOC-команди, рівень автоматизації). Це дає змогу організації не лише оцінити власну захищеність, а й визначити напрями інвестування у розвиток процесів, що підвищують загальну зрілість [20, с. 501–502].

На завершальному рівні інтеграції доцільно використовувати *KPI для вимірювання зрілості інформаційної безпеки.* Вони забезпечують формалізацію даних у кількісних показниках, що дає змогу проводити як динамічний моніторинг, так і бенчмаркінг між різними організаціями. Основні KPI, рекомендовані для віртуальних мереж, наведено у табл. 3.

Отож інтеграція методів технічного аналізу з моделями зрілості через використання KPI дає змогу створити комплексну систему оцінювання, що поєднує тактичні, процесні та стратегічні аспекти інформаційної безпеки. Такий підхід формує основу для управління кіберризиками в умовах високої динаміки віртуальних інфраструктур.

Таблиця 3

KPI для вимірювання зрілості інформаційної безпеки

KPI	Опис	Зв'язок із моделями зрілості
MTTD (Mean Time to Detect)	Середній час виявлення інциденту від моменту його виникнення	Відображає здатність організації реалізувати функції *Detect* (NIST CSF) та перехід від реактивного до проактивного рівня
MTTR (Mean Time to Respond/Recover)	Середній час реагування та відновлення після інциденту	Відповідає рівню процесної зрілості реагування (Respond/Recover у NISTCSF)
% автоматизації	Частка автоматизованих процедур (SOAR, SIEM-плейбуки) у загальному обсязі операцій	Є критерієм переходу від базових до оптимізованих рівнів зрілості (Managed/Optimized)
Кількість хибнопозитивів (False Positives Rate)	Відсоток некоректно класифікованих інцидентів	Демонструє якість процесів кореляції подій та зрілість інтелектуальних систем виявлення
Patch Management Coverage	Частка систем, де своєчасно застосовано критичні оновлення	Характеризує інтеграцію технічного контролю з управлінськими процесами
Security Awareness Index	Відсоток співробітників, які пройшли тренінги з кібербезпеки	Відображає організаційний аспект зрілості та здатність до формування "людського бар'єра"

Практичні сценарії застосування в організаціях

Оцінка зрілості інформаційної безпеки у контексті віртуалізованих інфраструктур набуває особливого значення для організацій, які функціонують у режимі високої залежності від цифрових сервісів. Практичні сценарії її використання демонструють, як поєднання технічних метрик та процесних характеристик трансформується у стратегічні інструменти управління ризиками.

V. Tsurkan, O. Shapoval вказують на те, що одним із показових напрямів є оцінка зрілості у великих корпораціях та державних структурах. У таких організаціях застосування моделей типу NIST CSF чи SSE-CMM дає змогу співвіднести фактичний рівень автоматизації та процесної керованості із нормативними вимогами та галузевими стандартами. Наприклад, у великих банківських чи телекомунікаційних компаніях формуються комплексні матриці зрілості, де результати пентестів і аналізу уразливостей інтегруються з управлінськими метриками (наявність SOC, час реагування, охоплення patch management). У державному секторі оцінка зрілості часто використовується для визначення готовності до відповідності стандартам кіберзахисту та критичної інфраструктури [19, с. 211].

Другим важливим прикладом є розробка дашбордів зрілості на основі даних SIEM / SOAR. Такі дашборди виконують роль інтеграційних інструментів, які в реальному часі відображають технічні (MTTD, MTTR, false positives), процесні (ступінь автоматизації реагування, відповідність сценаріїв playbooks) та організаційні показники (рівень обізнаності персоналу, кількість інцидентів, що потребували ескалації). Вони стають практичним відображенням моделей зрілості: наприклад, на рівні "Adaptive" у NIST CSF передбачається не лише вимірювання KPI, але й їхня візуалізація у вигляді метрик для прийняття управлінських рішень. Таким чином, дашборди виступають практичним мостом між технічними системами моніторингу та стратегічними моделями зрілості [4, с. 2149].

R. Sardar вважає, що окремої уваги заслуговує питання визначення "больових точок" для компаній різного масштабу. Для малих і середніх підприємств критичними є фінансові обмеження та дефіцит кваліфікованого персоналу, що призводить до низького рівня автоматизації та високої залежності від ручних процедур. У великих корпораціях навпаки, "больовими точками" є складність узгодження процесів між підрозділами, надлишкова бюрократизація та ризик дублювання процедур. Для державних структур ключовою проблемою є поєднання високих вимог до захисту критичних систем з обмеженою гнучкістю регуляторного середовища. Ідентифікація цих особливостей дає змогу адаптувати методи оцінки зрілості та спрямовувати ресурси на оптимізацію найвразливіших сегментів.

Важливим аспектом у подоланні зазначених “больових точок”, на думку K. S. Chandan, є використання адаптивних моделей зрілості, здатних масштабуватися відповідно до ресурсних можливостей організації. Для малих компаній доцільним є застосування спрощених рамок із базовим рівнем автоматизації та акцентом на навчанні персоналу, тоді як великі корпорації можуть впроваджувати комплексні системи SOAR та інтегровані KPI, що охоплюють процеси виявлення й реагування. Державним структурам варто зосереджуватися на гармонізації вимог регуляторів з міжнародними стандартами, щоб уникнути дублювання контрольних заходів і забезпечити узгодженість між різними відомствами [10].

Додаткову складність створює швидка еволюція технологій та загроз, яка підсилює навантаження на всі категорії організацій незалежно від масштабу. У цих умовах “больові точки” трансформуються, наприклад, брак кадрів стає ще відчутнішим через необхідність знань у сфері хмарних сервісів, контейнеризації та ШІ-рішень. Це зумовлює потребу у гнучких підходах до підготовки фахівців і створення спільних центрів компетенцій, здатних обслуговувати кілька організацій одночасно. Такий підхід сприяє зниженню витрат, підвищенню якості впровадження зрілісних моделей і формуванню стійкої кіберекосистеми на міжорганізаційному рівні [18].

Отже, практичні сценарії застосування моделей зрілості підтверджують їхню подвійність: з одного боку, вони є формалізованими інструментами аудиту та контролю, а з іншого – слугують основою для гнучкого управління кіберризиками з урахуванням масштабів, ресурсних можливостей та стратегічних цілей конкретної організації.

Виклики впровадження систем оцінки зрілості

Запровадження моделей оцінки зрілості інформаційної безпеки у віртуалізованих середовищах є складним процесом, що потребує врахування технологічних, кадрових та економічних факторів. Попри очевидні переваги у формалізації процесів управління ризиками, організації часто стикаються з низкою бар’єрів, які уповільнюють або навіть унеможливлюють ефективне впровадження. Для систематизації основних перешкод їх доцільно розглядати у трьох взаємопов’язаних площинах – технічній, кадровій та економічній (табл. 4) [5]. Водночас, коли керівництво недостатньо усвідомлює складність та ресурсні вимоги, може суттєво підвищувати ризик неефективності впровадження, що потребує ретельного планування та підтримки на всіх рівнях управління.

Таблиця 4

Ключові виклики впровадження систем оцінки зрілості

Категорія викликів	Сутність проблеми	Наслідки для організацій
Технічні	Проблеми сумісності рішень різних вендорів; складність інтеграції у мультихмарних середовищах; обмежена масштабованість наявних систем моніторингу	Фрагментація інфраструктури безпеки, втрата уніфікованих метрик, підвищення ризику “сліпих зон” у віртуальних мережах
Кадрові	Дефіцит фахівців із впровадження та експлуатації SOAR, недостатня кількість висококваліфікованих аналітиків SOC, перевантаження персоналу рутинними завданнями	Зниження ефективності процесів реагування, висока залежність від окремих спеціалістів, ризик затримки виявлення та усунення інцидентів
Економічні	Висока вартість комплексних платформ SIEM/SOAR/XDR; значні витрати на навчання персоналу та підтримку сертифікацій; обмежені бюджети малих і середніх компаній	Уповільнене впровадження моделей зрілості, вибір часткових або спрощених рішень, відсутність довгострокових програм розвитку кіберстійкості

Аналіз викликів впровадження систем оцінки зрілості демонструє, що вони мають багатовимірний характер і охоплюють як технічні аспекти інтеграції рішень у складні віртуальні інфраструктури, так і кадрові та економічні обмеження. У результаті формується асиметрія між

необхідністю підвищення рівня кіберстійкості та реальними можливостями організацій. Подолання цих бар'єрів можливе лише за умови комплексного підходу: розвитку міжвендорних стандартів сумісності, інвестування в підготовку кадрів та адаптації економічних моделей впровадження (наприклад, через використання SaaS-рішень або спільних кіберцентрів). Лише такий підхід дозволить забезпечити поступове й ефективне зростання зрілості інформаційної безпеки у віртуалізованих мережах [1, с. 35].

Отже, табл. 4 ілюструє комплексність викликів, з якими стикаються організації. Ефективне подолання цих бар'єрів потребує поєднання технічних рішень, інвестицій у розвиток людського капіталу та адаптації економічних моделей, що забезпечує не лише впровадження систем оцінки зрілості, а й їхню стійку інтеграцію у процеси управління кіберризиками.

Перспективи розвитку підходів до оцінки зрілості

Еволюція підходів до оцінювання зрілості інформаційної безпеки у віртуалізованих інфраструктурах рухається у бік даних-керованості, експериментальної перевірності та корпоративної ціннісної інтеграції. Три вектори – AI/L-прогнозування, цифрові двійники безпеки та ESG-інтеграція – формують нову методологічну рамку, у якій технічні метрики з'єднуються з процесними показниками та нефінансовими ризиками. Це дає змогу організаціям більш точно прогнозувати потенційні загрози, оптимізувати ресурси та інтегрувати оцінку кіберстійкості у стратегічне планування. Крім того, поєднання цих підходів сприяє підвищенню прозорості управлінських рішень та формує основу для безперервного вдосконалення процесів безпеки у динамічних IT-середовищах.

Штучний інтелект і машинне навчання для прогнозування атак.

AI/ML переводять оцінювання захищеності з постфактум-аудиту до проактивної предиктивної аналітики. Джерела даних: телеметрія SIEM/EDR/XDR, NetFlow/pcap, журнали гіпервізорів та оркестраторів, події ідентифікації/доступу (IAM), а також контекст активів (CMDB). Методологічно доцільні три класи моделей:

1. Послідовні та часові моделі (LSTM/GRU, Transformers для подій SOC): прогноз "ланцюжків подій" і ймовірності ескалації інцидентів.
2. Графові методи (GNN на графах мережевих взаємодій і графах ATT&CK): оцінка схильності до lateral movement, виявлення аномальних підграфів.
3. Непіднаглядні/напівнаглядні підходи (autoencoders, isolation forests): виявлення zero-day та слабосигнальних відхилень у динамічних сегментах VN / overlay [12].

Ключові вимоги зрілості AI-контурів:

– керування зсувом моделей (*model drift management*) – регулярне онлайн-оновлення та валідація алгоритмів;

– адверсаріальна стійкість – застосування методів захищеного навчання, протидія підміні та отруєнню навчальних даних;

– пояснюваність (explainability) – використання підходів SHAP, контрфактуального аналізу для ув'язки рішень моделей із процедурами NIST CSF (*Detect / Respond*);

– управління даними (*data governance*) – політики зберігання, анонімізації та балансування класів у вибірках.

У межах інтегрованих моделей зрілості доцільно запроваджувати нові індикатори:

– Predictive MTTD – прогнозований середній час виявлення інцидентів;

– Prevented Incidents Ratio – частка інцидентів, попереджених за допомогою ML-алертів;

– Coverage at Risk – відсоток критичних активів, для яких забезпечено предиктивний моніторинг [21, с. 605].

Цифрові двійники безпеки (Security Digital Twins).

Цифровий двійник безпеки – це синхронізована з продуктивним середовищем семантична модель активів, топологій (L2/L3, overlay/underlay, мікросегментація), політик доступу та бібліотеки

технік (MITRE ATT&CK), у якій можливе масштабне симулювання сценаріїв атак і контрзаходів без ризику для продакшну.

Функціональні блоки:

– Фіделіті-модель інфраструктури (включно з гіпервізорами, віртуальними комутаторами, east-west трафіком).

– Граф атак з вагами імовірностей/вартості (attack-path analysis, k-shortest paths до "цілей корони").

– Симулятори контролів (NGFW/IDS/EDR/SOAR playbooks) з часовою динамікою MTTD/MTTR.

– Калібрування за живою телеметрією (digital-physical loop) і байєсівське оновлення ризик-параметрів [6, с. 632].

Метрики зрілості DT-підходу: fidelity score (узгодженість з продакшном), scenario coverage (покриття критичних шляхів), time-to-mitigation@scenario, control efficacy uplift (дельта ризику до / після зміни політики). Практично це дозволяє досягти "*evidence-based maturity*": підвищення рівня зрілості підтверджується експериментально (purple-team у двійнику), а не декларативно.

ESG-інтеграція: кіберстійкість як компонента сталості.

ESG переносить оцінку зрілості за межі чисто технічних показників до управління нефінансовими ризиками та довіри стейкхолдерів. У фокусі:

1. G (Governance): прозорість кіберуправління (наявність комітету, частота звітності, аудит), ланцюг постачання (вимоги до постачальників за ISO/NIST), інцидент-трансформація в уроки (lessons learned).

2. S (Social): індекс обізнаності персоналу, політики приватності, безперервність критичних послуг для клієнтів/громадян.

3. E (Environmental): енергоефективність SOC/центрів обробки, "зелений" профіль хмарних контрольних заходів [2, с. 107].

Інтегрований ESG-Cyber Maturity Index може агрегувати: (i) відповідність ISO 27001/NIST CSF, (ii) показники безперервності та інцидент-прозорості, (iii) зрілість вимог до постачальників (third-party risk), (iv) тренінгові та культурні метрики. Такий індекс робить кіберстратегію порівнюваною у нефінансовій звітності, узгоджуючи безпеку з корпоративною стійкістю та репутаційним капіталом.

Поєднання AI/ML-прогнозування, експериментальної верифікації через цифрові двійники та ESG-інтеграції формує наступне покоління підходів до зрілості: від реактивної констатації стану до прогнозно-керованої, експериментально підтвердженої і соціально відповідальної кіберстійкості. Це зміщує мету оцінювання з "відповідності мінімумам" до стратегічної оптимізації ризику в умовах динаміки віртуальних мереж.

Результати дослідження

Проведене дослідження дало змогу сформувати цілісне уявлення про взаємозв'язок між методами технічної оцінки захищеності віртуальних мереж та процесними моделями зрілості інформаційної безпеки. По-перше, було встановлено, що класичні підходи – аналіз уразливостей, тестування на проникнення, моделювання загроз і кількісна оцінка ризиків – зберігають свою релевантність, проте їх ефективність значною мірою залежить від можливості інтеграції з процесними рамками, зокрема NIST CSF, SSE-CMM та гібридними моделями, що поєднують вимоги ISO / IEC 27001.

По-друге, доведено, що систематизація результатів технічних перевірок у форматі інтегрованих матриць дозволяє зіставляти тактичні метрики (MTTD, MTTR, відсоток автоматизації) з рівнями зрілості процесів управління ризиками. Це забезпечує перехід від реактивного реагування на інциденти до проактивного прогнозування та стратегічного планування захисту.

По-третє, дослідження виявило критичні виклики впровадження систем оцінки зрілості: технічні (інтеграція у мультихмарних середовищах, сумісність різновендорних рішень), кадрові

(дефіцит аналітиків SOC та інженерів SOAR), економічні (висока вартість комплексних платформ та навчання персоналу). Їх подолання можливе лише за умови розробки уніфікованих стандартів сумісності, розвитку освітніх програм та оптимізації економічних моделей впровадження (наприклад, через SaaS-рішення або регіональні центри кіберзахисту).

Нарешті, було окреслено перспективні вектори розвитку, які передбачають застосування штучного інтелекту та машинного навчання для прогнозування атак, впровадження цифрових двійників безпеки для моделювання сценаріїв та верифікації контролів, а також інтеграцію кібербезпеки у ширші ESG-стратегії корпоративної стійкості. Це дає змогу розглядати зрілість інформаційної безпеки не лише як технічну характеристику, а й як елемент довгострокової конкурентоспроможності організацій [15; 16].

Висновки

Проведене дослідження дало змогу досягти поставленої мети – розробити науково обґрунтований підхід до оцінювання захищеності віртуальних мереж у поєднанні з моделями зрілості інформаційної безпеки. Було показано, що класичні методи технічної перевірки (аналіз уразливостей, тестування на проникнення, моделювання загроз, кількісна оцінка ризиків) зберігають актуальність, однак їхня ефективність істотно зростає у разі інтеграції з процесними моделями зрілості (NIST CSF, SSE-CMM, ISO/IEC 27001).

У межах дослідження наведено приклад інтегрованої матриці оцінювання, що містить кількісні показники MTTD (14 год), MTTR (36 год), рівень автоматизації (42 %), Patch Management Coverage (78 %) та Security Awareness Index (65 %). Ці дані продемонстрували, що організація досягає середнього рівня зрілості, проте має критичні “вузькі місця” у швидкості реагування, управлінні оновленнями та рівні підготовки персоналу. Зведення отриманих чисельних характеристик у єдину систему підтвердило доцільність застосування інтегрованих метрик для стратегічного управління ризиками. Отже, поставлену мету дослідження виконано.

Практична значущість результатів полягає у створенні інструментарію, який можуть використовувати організації для комплексної оцінки кіберстійкості, обґрунтування інвестицій у безпеку, вибору пріоритетних напрямів розвитку систем захисту та підвищення ефективності управлінських рішень у сфері інформаційної безпеки.

Подальші дослідження доцільно спрямувати на удосконалення предиктивних моделей оцінювання зрілості на основі штучного інтелекту, впровадження цифрових двійників безпеки для експериментальної перевірки захисних заходів, а також на розробку ESG-орієнтованих підходів, які інтегрують кіберстійкість у стратегії корпоративного управління. Реалізація таких напрямів дасть змогу сформувати нову парадигму оцінювання зрілості інформаційної безпеки, що поєднує технологічну ефективність, управлінську гнучкість та стратегічну цінність для суспільства і держави.

Список літератури

1. Гребенніков А. Б., Щебланін Ю. М. Аналіз використання моделей зрілості процесів в ході оцінювання рівня інформаційної безпеки. Сучасний захист інформації. 2018. (1). 33–37. URL: http://nbuv.gov.ua/UJRN/szi_2018_1_8.

2. Сторчак А., Сальник С. Метод оцінювання рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз. Системи обробки інформації. 2019. (3). 98–109. DOI: https://doi.org/10.30748/soi.2019.158.12.

3. Acheampong R., Popovici D.-M., Balan T. C. A cybersecurity risk assessment for enhanced security in virtual reality. Information. 2025. 16(6). DOI: https://doi.org/10.3390/info16060430.

4. Agnew D., Boamah S., Bretas A., McNair J. Network security challenges and countermeasures for software-defined smart grids: A survey. Smart Cities. 2024. 7(4). 2131–2181. DOI: https://doi.org/10.3390/smartcities7040085.

5. Altulaihan E., Almaiah M. A., Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics. 2022. 11(20). DOI: https://doi.org/10.3390/electronics11203330.

6. Anass R., Saliha A., Khadija O. T., Ounsa R. Information and cyber security maturity models: A systematic literature review. Information and Computer Security. 2020. 28(4). 627–644. DOI: https://doi.org/10.1108/ICS-03-2019-0039.

7. Bays L. R., Oliveira R. R., Barcellos M. P. et al. Virtual network security: Threats, countermeasures, and challenges. Journal of Internet Services and Applications. 2015. 6(1). DOI: https://doi.org/10.1186/s13174-014-0015-z.

8. Bernardo L., Malta S., Magalhães J. An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics. 2025. 14(7). DOI: https://doi.org/10.3390/electronics14071364.

9. Brezavšček A., Baggia A. Recent trends in information and cyber security maturity assessment: A systematic literature review. Systems. 2025. 13(1). DOI: https://doi.org/10.3390/systems13010052.

10. Chandan K. S. (n.d.). Network security testing: Types, tools, techniques. URL: https://qualysec.com/network-security-testing/.

11. Domínguez-Dorado M., Calle-Cancho J., Galeano-Brajones J. Detection and mitigation of security threats using virtualized network functions in software-defined networks. Applied Sciences. 2024. 14(1). DOI: https://doi.org/10.3390/app14010374.

12. Hochstetter-Diez J., Diéguez-Rebolledo M., Fenner-López J., Cachero C. AIM triad: A prioritization strategy for public institutions to improve information security maturity. Applied Sciences. 2023. 13. DOI: https://doi.org/10.3390/app13148339.

13. Khudyntsev M. M., Palazhchenko I. L. Cybersecurity maturity models for cybersecurity assessment in critical infrastructure. Environmental Safety and Natural Resources. 2024. 52(4). 122–134. DOI: https://doi.org/10.32347/2411-4049.2024.52.4.122-134.

14. Knowles M. (n.d.). Cybersecurity risk management: Frameworks, plans, and best practices. URL: https://hyperproof.io/resource/cybersecurity-risk-management-process/.

15. Muronga K., Herselman M., Botha A., Da Veiga A. An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A scoping review. Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp) (pp. 1–6). Balaclava, Mauritius. 2019, November.

16. Papachristofis K., Vardoulias G., Vavousis K. Comparative evaluation of cybersecurity maturity models and frameworks. In Information Systems. EMCIS 2024. Lecture Notes in Business Information Processing. 2025. (Vol. 536). Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-81325-2_12.

17. Pasdar A., Koroniotis N., Keshk M. Cybersecurity solutions and techniques for Internet of Things integration in combat systems. IEEE Transactions on Sustainable Computing. 2024. 10. 1–20.

18. Sardar R., Anees T., Al-Shamayleh A. S. et al. Challenges in detecting security threats in WoT: A systematic literature review. Artificial Intelligence Review. 2025. 58. DOI: https://doi.org/10.1007/s10462-025-11176-z.

19. Tsurkan V., Shapoval O. Analysis of computer network security risk assessment methods. Information Technology and Security. 2022. 10(2). 204–215. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270437.

20. Wei H., Zhao X., Shi B. Research on neural networks in computer network security evaluation and prediction methods. International Journal of Knowledge-Based and Intelligent Engineering Systems. 2024. 28(3). 497–516. DOI: https://doi.org/10.3233/KES-230407.

21. Ying Z., Li Q., Meng S. et al. A survey of information intelligent system security risk assessment models, standards and methods, in cloud computing, smart grid and innovative frontiers in telecommunications. In Innovative Frontiers in Telecommunications. 2020. (Vol. 322, pp. 603–611). Cham: Springer. DOI: https://doi.org/10.1007/978-3-030-48513-9_48.

22. Zhou W. Application exploration of virtual network technology in computer network security. Journal of Artificial Intelligence and Information. 2025. 2. 177–182.

METHODS FOR ASSESSING THE SECURITY OF VIRTUAL NETWORKS AND INFORMATION SECURITY MATURITY MODELS

O. Yu. Kotliarov, L. L. Bortnik

Lviv Polytechnic National University,
Department of Information Security

The article presents a comprehensive analysis of methods for assessing the security of virtual networks and their relationship with information security maturity models. Key technical approaches are considered-vulnerability analysis, penetration testing, threat modeling, and quantitative risk assessment-taking into account the specifics of multi-cloud and dynamic environments. It is demonstrated that combining these methods with process models (SSE-CMM, NIST Cybersecurity Framework, and hybrid approaches based on ISO/IEC 27001) enables the development of a multidimensional system for evaluating cyber resilience. Special attention is given to the construction of integrated assessment matrices that combine technical, organizational, and managerial metrics (MTTD, MTTR, level of automation, and patch management coverage).

The study highlights practical scenarios of applying maturity models in large corporations and government institutions, analyzing typical implementation "pain points"-technical (integration in multi-cloud environments, compatibility of heterogeneous solutions), staffing (shortage of highly qualified SOC/EDR/SOAR specialists), and economic (high cost of platforms and staff training). Current development trends are summarized, including the use of artificial intelligence and machine learning for attack prediction, the application of cybersecurity digital twins as a tool for experimental verification of controls, and the integration of ESG strategies to enhance corporate resilience.

The obtained results provide a foundation for unified methodologies for assessing organizational maturity and cyber resilience, enable the combination of technical and strategic dimensions of information security, and support the transition from reactive incident response to proactive risk management.

Keywords: virtual networks, security assessment, information security maturity models, quantitative risk assessment, cyber resilience, artificial intelligence.