КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.731
УДК 004.056

Палко Дмитро Володимирович
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-2886-1975
palko.dmytro@gmail.com

Мирутенко Лариса Вікторівна
кандидат технічних наук, доцен
доцент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0003-1686-261X
myrutenko.lara@gmail.com

МЕТОД КОМПЛЕКСНОЇ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анотація. Оцінка та аналіз ризиків кібербезпеки є важливим елементом для побудови ефективної системи управління ІБ. Висока складність та масштабованість архітектури сучасних розподілених систем, різнорідність обладнання та інфраструктури, а також постійні зміни конфігурації та масштабування середовища породжують ряд проблем, пов'язаних зі збором та аналізом інформації для оцінки ризиків, необхідністю оперативної обробки великих масивів складних за структурою та гетерогенних за природою даних, що надходять із диференційованих систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел, а також відсутністю єдиного формату їх представлення. Обмеженість наявних стандартів та методологій в динамічних умовах сучасних РІС, їх концептуальний характер і складність практичної імплементації та застосування, вимагає розробки гнучких методологічних та технологічних рішень для аналізу кіберризиків, які б інтегрували переваги існуючих підходів, забезпечували автоматизацію обчислень і враховували динамічні аспекти розподіленого середовища. У дослідженні представлено комплексний адаптивний метод кількісної оцінки ризиків кібербезпеки в розподілених інформаційних системах, що є актуальним з точки зору забезпечення ефективності застосування в динамічних умовах складних багатокомпонентних та масштабованих РІС. Запропонований метод, інтегруючи метрико-орієнтовний підхід на основі врахування результатів комплексу нейромережевих моделей оцінки безпекових показників стану інфраструктури РІС та метрик контролю відповідності нормативно-правовій базі і вимогам провідних стандартів ІБ, надає можливість створити масштабовану та динамічну систему управління кіберризиками, що ефективно реагує на сучасні загрози в РІС та відкриває можливості для комплексного впровадження інтелектуальних систем управління інформаційною безпекою в процеси ризик-менеджменту.

Ключові слова: кібербезпека; інформаційна безпека; ризик інформаційної безпеки; оцінка ризиків; управління ризиками; розподілена інформаційна система; нейронна мережа.

ВСТУП

Сучасні розподілені інформаційні системи (РІС) є основою для функціонування складних інформаційно-комунікаційних інфраструктур, охоплюючи хмарні середовища, інтернет речей (IoT), корпоративні мережі та важливі об'єкти критичної інфраструктури. Зі зростанням масштабів та гетерогенності таких систем підвищуються вимоги до ефективних методів оцінки ризиків кібербезпеки, що враховують динамічний характер

середовища, високу варіативність конфігурацій та постійні зміни ландшафту потенційних загроз [1].

Стрімкий розвиток цифрових технологій та постійне розширення архітектури розподілених інформаційних систем зумовлює високу складність керування їхньою безпекою. Висока гетерогенність апаратного та програмного забезпечення, динамічність мережевих топологій, активне впровадження хмарних платформ та мікросервісних архітектур, а також значне різноманіття інформаційних активів створюють додаткові труднощі в оцінці ризиків інформаційної безпеки (ІБ) [2-3]. Окрім того, оцінювання ризиків кібербезпеки в розподілених системах потребує врахування таких особливостей, як функціональна розподіленість, ієрархічна організація, висока ступінь паралелізму обчислень і майже повна відсутність централізованого управління [4].

Зростання складності РІС і водночас підвищення значущості інформаційної безпеки для стратегічного розвитку організацій вимагають нових підходів до оцінки ризиків, здатних оперативно реагувати на динамічні зміни оточення і забезпечувати високий рівень точності та надійності аналізу, долаючи обмеження класичних підходів.

Паралельно з цим відзначається значне зростання кількості та складності кіберзагроз. Зловмисники активно використовують розподілену природу сучасних РІС для поширення шкідливого програмного забезпечення, проведення DoS та DDoS-атак, викрадення або модифікації конфіденційних даних.У результаті, безпекові виклики набувають нових форм, а традиційні механізми захисту стають недостатніми, адже вони були розроблені переважно для централізованих та однорідних систем. Це зумовлює необхідність пошуку та впровадження більш гнучких, динамічних і інтелектуальних підходів до забезпечення кібербезпеки, які б могли виявляти та реагувати на загрози в режимі реального часу, а також ефективно оцінювати ризики, пов’язані з вразливостями та атаками на масштабовані розподілені інфраструктури. [5]

Постановка проблеми. Сучасні методології оцінки ризиків ІБ та стандарти з ризик-менеджменту (в першу чергу ISO/IEC 27005:2022 та NIST SP 800-30) в переважній більшості носять концептуальний характер та засновані на класичних статистичних підходах до обрахунку рівня ризику, що є малоефетивним в умовах РІС.

До основних викликів оцінки ризиків в розподіленому середовищі можна віднести:

- Високу складність та масштабованість систем: різнорідність обладнання та інфраструктури; динамічну природа середовища; постійні зміни в конфігурації та масштабування; великий обсяг трафіку, що ускладнює моніторинг усіх компонентів;
- Проблему збору та аналізу даних для оцінки ризиків: необхідність оперативної обробки великих масивів складних за структурою та гетерогенних за природою даних, що надходять із диференційованих систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел; відсутність єдиного формату представлення даних у різних системах; складність агрегування, потреба у низькій затримці аналізу;
- Відсутність єдиних стандартів та методологій: відсутність універсального підходу, що враховував би специфіку розподілених систем, мав би уніфіковані метрики аналізу ризику для порівняння між різними середовищами, та легко адаптувався б до динамічних змін середовища та ландшафту загроз.
- Низьку ефективність традиційних методів у розподілених середовищах: Класичні підходи засновані на методах експертних оцінок, статистичному аналізі чи імітаційному моделюванні виявляють низку обмежень у

масштабованому та динамічному середовищі PIC і підкреслюють ряд важливих науково-прикладних проблем.

Таким чином, існуючі підходи до оцінки ризиків ІБ не в змозі повною мірою створити умови для забезпечення ефективного процесу ризик-менеджменту з урахуванням сучасних вимог та реалій функціонування розподілених середовищ [6-8].

Аналіз останніх досліджень і публікацій. Оцінка ризиків кібербезпеки є одним із ключових напрямів досліджень у сфері інформаційної безпеки, оскільки дозволяє виявляти, класифікувати та мінімізувати потенційні загрози для розподілених інформаційних систем (PIC). Відповідно до стандарту NIST SP 800-30, цей процес ґрунтується на систематичному підході до виявлення загроз, вразливостей та потенційних наслідків для організації, що дозволяє приймати обґрунтовані рішення щодо заходів захисту [9].

Одним із найпоширеніших підходів до оцінки критичності вразливостей є система Common Vulnerability Scoring System (CVSS), запропонована Forum of Incident Response and Security Teams (FIRST) [10]. CVSS забезпечує уніфікований підхід до оцінювання впливу вразливостей на систему, проте має ряд обмежень, серед яких відсутність врахування контексту середовища, недостатня адаптивність до динамічних змін, а також ігнорування взаємозв'язків між активами. У роботі [11] пропонується кількісна методологія, заснована на CVSS, що спрямована на надання більш детального та точного підходу до оцінки ризиків, враховуючи як характеристики активів, так і специфіку вразливостей, що дозволяє організаціям проводити більш обґрунтовану та точну оцінку ризиків інформаційних систем.

Інший підхід до оцінки ризиків базується на ймовірнісних моделях, які дозволяють визначати ризики на основі статистичного аналізу та історичних даних. У роботі [12] застосовано байєсівські мережі для прогнозування ризиків у корпоративних мережах. Метод демонструє високу ефективність для оцінки сценаріїв атак, але вимагає значних обчислювальних ресурсів для навчання моделей.

Методи Монте-Карло, як зазначено у дослідженні [13], використовуються для моделювання сценаріїв атак і оцінки їхнього впливу на систему. Проте їхня ефективність значною мірою залежить від точності вихідних даних та обмежень обчислювальної потужності.

Застосування методів нечіткої логіки в оцінці ризиків дозволяє адаптивно обробляти невизначені дані та враховувати контекст середовища. Наприклад, у дослідженні [14] запропоновано методологію оцінки ризиків на основі нечіткої моделі логічного виводу, що дозволяє коригувати рівень загроз залежно від важливості активів.

Методи машинного навчання використовуються для автоматизації процесу виявлення та аналізу загроз. У роботі [15] автор пропонує нейромережевий підхід, що базується на кількісній оцінці ризиків з урахуванням великої кількості взаємодіючих пристроїв. Проте такі методи вимагають великих обсягів навчальних даних та можуть бути складними в імплементації.

Сучасні дослідження також орієнтовані на автоматизацію процесу оцінки ризиків у розподілених середовищах. У дослідженні [16] запропоновано комплексний гібридний підхід, який передбачає використання комплексу моделей оцінки для створення адаптивної системи проведення всебічного аналізу ризиків з метою покращення процесів підтримки прийняття рішень. Дослідження демонструє, що такий підхід дозволяє динамічно коригувати рівень ризику відповідно до змін конфігурації системи.

Важливим напрямом є інтеграція систем управління ризиками з Security Information and Event Management (SIEM) та Security Orchestration, Automation, and Response (SOAR),

як зазначено у [17]. Такі рішення дозволяють оперативно аналізувати події безпеки та автоматизувати реакцію на загрози.

Таким чином, аналіз наукових праць свідчить про наявність значних обмежень для задач оцінки в умовах сучасних РІС, що в свою чергу вимагає розробки адаптивного методу комплексної оцінки ризиків, який би інтегрував переваги існуючих підходів, забезпечував автоматизацію обчислень і враховував динамічні аспекти розподіленого середовища.

Незважаючи на значну кількість публікацій, що присвячені питанням оцінки ризиків кібербезпеки, розробка наукових і методологічних основ створення комплексного та адаптивного підходу до оцінки ризику в РІС залишається актуальним науково-прикладним завданням.

Метою статті є формування переліку вимог та напрацювання комплексних методологічних та технологічних рішень для оцінки ризиків кібербезпеки в РІС (з урахуванням специфіки функціонування динамічних розподілених середовищ), що здатні підвищити ефективність, точність та адаптивність аналізу, покращити здатність протидіяти сучасним кіберзагрозам та забезпечити сталий розвиток у цифровому середовищі і безперервне підвищення зрілості у сфері ІБ.

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

Оцінка ризиків кібербезпеки в умовах розподілених середовищ, є складним, багатофакторним процесом, оскільки передбачає вирішення комплексу проблем, що пов’язані з розподіленістю інфраструктури, динамічним характером загроз, зростанням вимог регуляторів та суттєвою обмеженістю існуючих методологій та підходів до оцінювання ризиків в умовах масштабованих РІС. Це в свою чергу, створює передумови до пошуку нових методологічний та практичних механізмів аналізу, та вимагає розробки комплексної та адаптивної методології оцінки кіберризиків в РІС, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища і ймовірнісний характер кіберзагроз, сприяє підвищенню зрілості процесів кібербезпеки та дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

Основні вимоги до запропонованої методології можна узагальнити в наступних ключових положеннях та принципах:

- Комплексність та універсальність: Облік множинних факторів ризику, включаючи технічні, організаційні та нормативно-правові аспекти; застосовність до різних типів ІТ-активів, що можуть значно диференціюватись за характером, призначенням та технічними аспектами функціонування (архітектура, обладнання, протоколи взаємодії тощо);
- Масштабованість: Здатність ефективно аналізувати масштабовані розподілені системи та асоційовані з їх функціонуванням великі масиви різнорідних даних;
- Гнучкість та адаптивність: Можливість динамічної корекції оцінки ризику та адаптації до змін середовища без необхідності повторного навчання моделей; спроможність гнучко підлаштовуватись до змін умов функціонування, розмірів, топології та архітектури інфраструктури;
- Автоматизованість та практична орієнтація: Орієнтація на практичні аспекти імплементації та застосування з можливістю реалізації автоматизованих сценаріїв оцінки.

Таким чином, розроблена методологія повинна бути побудована на принципах комплексної оцінки із врахуванням всіх наявних даних та метрик безпеки, а також кореляції з існуючими факторами ризику, профілем потенційних загроз, та орієнтацією на аспекти практичної імплементації та застосування в корпоративному середовищі типової розподіленої інформаційної системи, створеної для забезпечення одного або декількох типів інформаційних процесів та / або надання інформаційних послуг. Окрім цього, розроблена модель повинна враховувати факт функціонування інформаційної системи в умовах невизначеності та ризику, при невідомих законах і числових характеристиках розподілу кіберзагроз [18].

З метою вирішення поставлених завдань та обмежень, запропоноване рішення об'єднує декілька важливих елементів:

– профіль ключових факторів ризику сучасних PIC, на основі якого проведено оптимізацію вхідного простору метрик для проектованих моделей [20];
– комплекс нейромережевих моделей оцінки ризику на основі аналізу агрегованих метрик розподіленого середовища [21-22];
– адаптивний метод кількісного оцінювання ризику на основі спроектованих моделей та загальної системи оцінки вразливостей CVSS (Common Vulnerability Scoring System).

Відсутність на сьогоднішній день стандартизованих методик аналізу захищеності розподілених інформаційних систем вносить момент невизначеності при прийнятті управлінських рішень та суб'єктивності в залежності від ситуації при визначенні необхідних і достатніх заходів безпеки та механізмів захисту. Формальні підходи до оцінювання, що включають експертний аудит, інвентаризацію, аналіз конфігурацій та налаштувань, перевірку відповідності корпоративним політикам, міжнародним стандартам чи нормативним документам, а також технічні аспекти пов'язані з пошуком та ідентифікацією наявних вразливостей, мережевим скануванням, перевіркою веб-додатків, або ж тестуванням на проникнення є ефективними механізмами аналізу поточного стану, проте з іншого боку передбачають розрізнений підхід з оцінкою вузького спектру безпекових аспектів, що притаманні предметній області кожного з методів. Окрім цього, перелічений інструментарій найчастіше застосовується окремо, а отже не забезпечує комплексного погляду на стан забезпечення безпеки в розподіленому середовищі. Варто зазначити, що аналіз результатів по деяким з описаних підходів дозволяє безпосередньо судити про стан забезпечення безпеки системи (наприклад навність вразливостей), тоді як інші лише опосередковано впливають на оцінку цього показника (відсутність політик ІБ, невідповідність вимогам стандартів тощо). Важливим аспектом даного питання є також необхідність забезпечення інтегральної оцінки ризиків в розрізі часу, що дозволить проводити порівняння рівня захищеності та приймати рішення щодо впроваджених механізмів захисту.

Одним із засобів формальної оцінки безпеки можуть бути метрики ІБ. За своєю суттю, метрики безпеки — є універсальним формалізованим критерієм для оцінки стану безпеки інформаційної системи та важливим механізмом управління та контролю. Поняття «метрики безпеки» передбачає застосування кількісного, статистичного та / або математичного аналізу для вимірювання ключових показників безпеки, в тому числі виражених у фінансовому еквіваленті потенціних втрат чи вартості відновлення компонентів системи. Таким чином, можна виділити набір універсальних атрибутів, що будуть актуальними для будь-якої розподіленої системи та в сукупності зможуть охарактеризувати рівень захищеності об'єкту чи IT-активу. Метрика безпеки (або їх

комбінація) являє собою кількісну міру відповідного атрибуту, яким даний об'єкт володіє.

Можна виділити наступні критерії вибору метрик безпеки:

- актуальність для прийняття рішення;
- простота виміру та агрегації — доступність для обрахунку та аналізу, можливість автоматизації перевірки та контролю;
- об'єктивність оцінки та відтворюваність — незалежність та відсутність впливу суб'єктивних чинників (наприклад експертних рішень)
- вимірюваність — можливість однозначної інтерпретації (переважно кількісної) та порівняння;

Для типової розподіленої інформаційної системи можна виділити широкий спектр стандартизованих метрик безпеки та інтегрованих показників, що забезпечать можливість моніторингу, контролю та подальшого аналізу стану системи [19].

Прикладами таких показників для окремого інформаційного / мережевого активу можуть бути:

- тип та категорія пристрою;
- тип, версія та номер збірки операційної системи;
- тип розгортання пристрою (фізичний / віртуалізація);
- кількість виявлених вразливостей;
- тип середовища функціонування активу (продуктивне, тестове тощо);
- наявність зареєстрованих інцидентів ІБ в минулому (врахування ретроспективних даних);
- дата-час останньої активності об'єкту;
- наявність та тип антивірусного ПЗ;
- дата-час останнього оновлення сигнатур / агента;
- статус застосування політик ІБ;
- статус підключення об'єкту до SIEM / DLP тощо;
- дата-час останнього сканування вразливостей.

Слід зазначити, що такі параметри можуть мати різні джерела походження, тип даних та формат представлення, що вимагає додаткового інструментарію аналітичного опрацювання.

Відбір метрик безпеки має враховувати аспекти комплексної оцінки, уніфікації процедури аналізу та врахування актуальних факторів ризику, що притаманні розподіленому середовищу. Для цього пропонується застосувати побудований профіль ключових факторів ризику сучасних РІС, що можуть спричинити потенційні інциденти ІБ в умовах фізичної та функціональної розподіленості ресурсів. Запропонований профіль забезпечує системний підхід до аналізу факторів ризику, ідентифікації впливу загроз і як результат — підвищення стійкості розподілених систем до можливих атак.

Окрім цього, він враховує кореляційний аналіз та моделювання взаємозв'язків факторів ризику, а також визначає та структурує основні заходи та контролі інформаційної безпеки, які демонструють найкращі показники ефективності в умовах розподіленості середовища, враховуючи як технологічні, так і організаційні аспекти.

Необхідність ідентифікації та попереднього аналізу основних факторів ризику, встановлення їх взаємозв'язків та кореляційних залежностей, безпосередньо пов'язана з якістю підготовки вхідних даних для побудови архітектури ефективних моделей глибокого навчання. Попередній етап статистичного дослідження та оцінки факторів ризику дозволяє оптимізувати вибір важливих інформативних ознак (feature selection). Виділення найсуттєвіших факторів ризику та контролів безпеки сприяє зменшенню

розмірності вхідних даних і мінімізує «шум», що у кінцевому підсумку покращує збіжність і стабільність процесу навчання нейронних мереж. Це особливо актуально для глибинних архітектур, де надмірна кількість ознак може призвести до складнощів оптимізації та ризику перенавчання (overfitting) [20].

Ключовим елементом запропонованого рішення, що забезпечує принцип комплексного аналізу та дослідження різних аспектів оцінки захищеності розподіленої системи є можливість використання комплексу нейромережевих моделей оцінки ризику [21-22].

Передумовою використання інструментарію машинного навчання та штучних нейронних мереж (та зокрема парадигми глибокого навчання) є:

- наявність невизначеності, обумовленої динамічною природою РІС;
- необхідність аналізу великих масивів складних значною мірою диференційованих даних та безпекових метрик про роботу РІС, агрегованих в процесі їх моніторингу;
- необхідність пошуку нелінійних залежностей і прихованих патернів в різнорідних гетерогенних даних, а також постійного покращення результатів аналізу завдяки здатності таких моделей навчатись та розпізнавати раніше невідомі сигнатури;
- необхідність практичного інструментарію та автоматизації процедури оцінки, що надасть можливість оперативного аналізу в режимі часу близькому до реального.

Моделі на основі алгоритмів машинного навчання та глибокий нейронних мереж, у порівнянні із класичними підходами до оцінювання ризиків ІБ, демонструють чудові якісні показники ефективності. Комплексне застосування декількох моделей забезпечує грунтовний системний підхід до оцінювання стану безпеки, враховуючи всі фактори та аспекти функціонування РІС, аналізуючи всі доступні дані та об'єднуючи їх результати в єдиному аналітичному середовищі.

Виходячи із вимог універсальності застосування, гнучкості оцінювання та комплексності аналізу запропоновано адаптивний метод трансформації якісної шкали оцінювання ризику в кількісний показник, що на відміну від класичного підходу враховує динамічний характер розподіленого середовища, та дозволяє автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

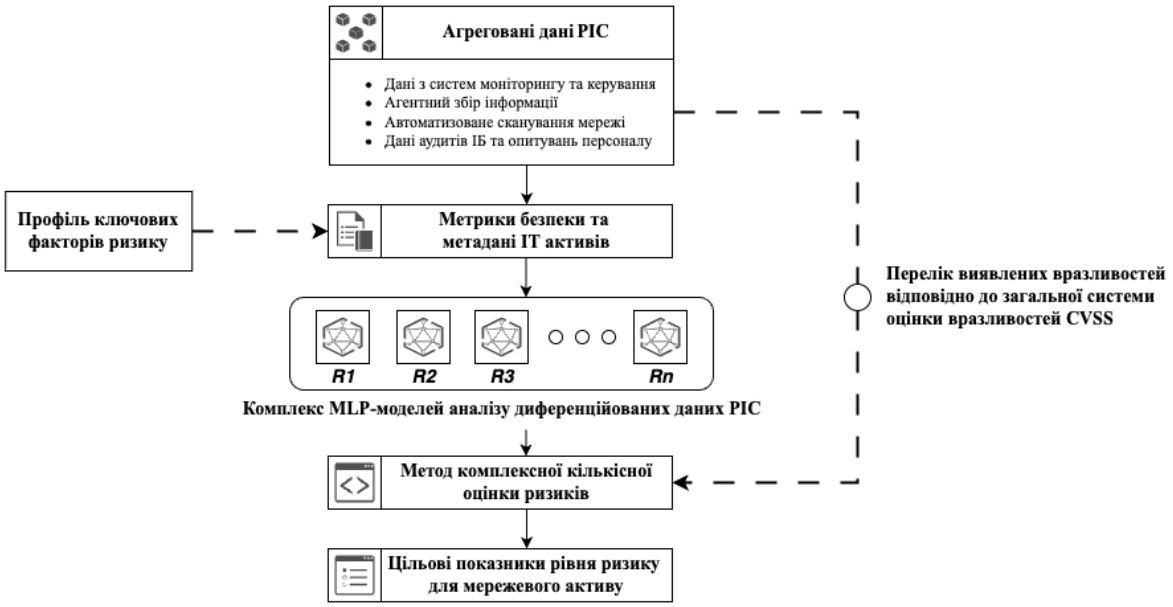

Рис. 1. Концептуальна схема комплексної методології оцінки ризику РІС

Як продемонстровано на рис. 1 в якості параметрів методу комплексної кількісної оцінки ризику розглядаються: множина об'єктів розподіленої системи (A), множина кібернетичних загроз (T) та множина виявлених вразливостей (V). Окрім цього, запропоноване рішення має враховувати диференційований рівень збитку при реалізації кібернетичних загроз для різних типів активів на основі проведеного профілювання за рівнем важливості та критичності об'єкту для інфраструктури (W_i).

Подальше обгрунтування потребує попередньої математичної формалізації.

Позначимо множину факторів ризику $F = \{F_1, F_2, \dots, F_i\}$, де F_i — фактор, який характеризує певний аспект стану безпеки інформаційної системи (наприклад, актуальність оновлень, наявність антивірусного захисту тощо). Кожен фактор описується певними безпековими метриками:

$$F_i = \{m_{i1}, m_{i2}, \dots, m_{ij}\}, \qquad m_{ij} \in [0,1] \tag{1}$$

де m_{ij} — нормалізована метрика, яка характеризує фактор F_i.

Визначимо множину ризиків $R = \{R_1, R_2, \dots, R_m\}$. Кожен ризик може залежати від одного або декількох факторів m_{ij}, при цьому кожен фактор може бути притаманним та формувати різні вектори загроз:

$$R_j = f_j(F_1, F_2, \dots, F_n), \tag{2}$$

де f_j — функція залежності, що описує вплив факторів ризику на ризик R_j.

Розподілена система складається з компонентів $A = \{A_1, A_2, \dots, A_n\}$, де A_i — окремий мережевий актив. Кожен актив A_i має індивідуальний рівень ризику $R(A_i)$, який залежить від ідентифікованих для нього факторів ризику, загроз та вразливостей.

Ризик кібербезпеки в класичному розумінні можна визначити як функцію загроз, вразливостей та можливих наслідків. Формально це можна представити наступним чином:

$$R(A_i) = f(T, V, I), \tag{3}$$

де $R(A_i)$ — рівень ризику для активу A_i.

T — множина потенційних загроз ($T = \{T_1, T_2, \dots, T_n\}$);

V — множина потенційних вразливостей ($V = \{V_1, V_2, \dots, V_m\}$);

I — можливий вплив загрози на систему ($I = \{I_1, I_2, \dots, I_k\}$).

В загальному випадку загрози можуть бути обраховані через ймовірності їх реалізації:

$$P(T_i) = \frac{N_{\text{успішних атак}}}{N_{\text{спроб атак}}}$$

де $N_{\text{успішних атак}}$ — кількість зафіксованих атак певного типу на подібні активи за певний період часу (тобто кількість реалізованих загроз);

$N_{\text{спроб атак}}$— загальна кількість атак (за той же період).

Окрім цього, модель ризику може бути виражена як ймовірнісний продукт:

$$R(A_i) = P(T_n) \cdot P(V_m) \cdot I_k, \tag{4}$$

де $P(T_n)$ — ймовірність виникнення загрози;
$P(V_m)$ — ймовірність експлуатації вразливості;
I_k — вплив загрози на актив.

Надане представлення можна ускладнити з врахуванням диференційованих впливів кожного з аргументів. Загальна формула оцінки ризику для конкретного активу з урахуванням ймовірності загрози, впливу та критичності активу набуде наступного вигляду:

$$R(A_i) = W_i \cdot (P(T_n) \cdot I_T + P(V_m) \cdot I_V), \quad (5)$$

де I_T — критичність впливу загрози (Threat Impact);
I_V — серйозність впливу вразливості (Vulnerability Impact).

Таким чином, модель комплексної оцінки рівня ризику для компонентів системи може бути обчислена як агрегована оцінка на основі врахування факторів ризику, загроз та вразливостей. Окрім цього, для розподілених систем важливо враховувати динаміку ризиків в часі:

$$R(A_i) = \sum_{j=1}^{h}\left[w_j(t) \cdot f_j(F_1(t), F_2(t), \dots, F_n(t))\right] \cdot \sum_{j=1}^{n}\sum_{j=1}^{m} P(T_n \cdot V_m) \cdot I_k, \quad (6)$$

де w_j — ваговий коефіцієнт для ризику R_j;
$f_j(F_1, F_2, \dots, F_n)$ — функція оцінки конкретного ризику;
$P(T_n \cdot V_m)$ — імовірність експлуатації вразливості V_m загрозою T_n;
t — час, а $w_j(t)$, $F_n(t)$ — значення, що змінюються в часі.

Обрахунок загального рівня ризику розподіленої інформаційної системи набуде наступного вигляду:

$$R_{total} = \sum_{i=1}^{N} R(A_i) \cdot W_i, \quad (7)$$

де W_i — ваговий коефіцієнт активу A_i, що відображає міру його важливості у системі (наприклад, на основі критичності або функціональному навантаженні компонента).

Описані методологічні принципи обрахунку дозволяють сформувати комплексний адаптивний метод обрахунку кількісного показника рівня ризику для розподіленого сердовища. Запропонований метод грунтується на спроектованих моделях [20-22] як ключових критеріях оцінки потенційних загроз, та враховує динамічний характер розподіленого середовища, використовуючи загальну систему оцінки вразливостей CVSS (Common Vulnerability Scoring System) для аналізу наявних вразливостей активу. Таким чином, запропонований підхід дозволяє врахувати параметри критичності активу на основі профілювання типів об’єктів та визначення їх важливості, а також ряд безпекових показників, пов’язаних із виявленим переліком вразливостей, що в свою чергу співвідноситься з класичною схемою обрахунку показника ризику, яка була описана раніше. Окрім цього, запропонований метод є достатньо гнучким та універсальним, не залежить від типу, архітектури, топології чи розміру інформаційної системи, та дозволяє повністю автоматизувати обрахунок показника ризику в умовах невизначеності та роботи з великими масивами гетерогенних даних.

$$R_{Scaled} = \frac{\frac{1}{k}(R_{1+} R_2 + \cdots + R_k) + \alpha \cdot R_{old}}{1+\alpha} \cdot \frac{\sum_{j=1}^{N} CVSS_j}{2N} \cdot W_i + \beta, \quad (8)$$

де R_k —показник рівня ризику обрахований відповідно до метрико-орієнтовної моделі оцінки $R_k \epsilon[1,5]$;

k — кількість нейромережевих моделей оцінки;

R_{old} — усереднений показник рівня ризику обрахований за результатами k моделей на попередній ітерації оцінки (наявність зв'язку з ретроспективними даними);

$CVSS_j$ – показник CVSS-score j вразливості $CVSS_j \epsilon[1,10]$;

N – кількість вразливостей задетектованих на мережевому активі;

α – коефіцієнт важливості врахування ретроспективних даних $\alpha \epsilon[0,1]$;

β – коефіцієнт коригування для окремого активу;

W_i – рівень критичності (важливості) активу $W \epsilon[1,4]$.

Відповідно до принципу, запропонованого в роботі [19], для систем з адитивними показниками ефективності окремих елементів (тобто таких систем, кожен з елементів яких вносить певний незалежний вклад в загальний результуючий ефект) сумарна ефективність може бути розрахована за формулою:

$$E(t) = \sum_{i=1}^{N} \sigma_i \cdot r_i(t), \quad (9)$$

де σ_i — вклад, що вноситься i-м елементом в сумарний вихідний ефект;

$r_i(t)$ — досліджуваний показник.

Таким чином, запропонований механізм за рахунок наявності коефіцієнту σ_i дозволяє врахувати зважені результати окремих моделей в залежності від їх пріоритету та важливості результату. Кожна з моделей здійснює якісну оцінку показника ризику відповідно до своєї предметної області за допомогою наступної шкали:

- Критичний — $r_i(t) = 5$;
- Високий — $r_i(t) = 4$;
- Середній — $(r_i(t) = 3$;
- Низький — $r_i(t) = 2$;
- Інформаційний — $r_i(t) = 1$;

Окрім цього, за рахунок наявності коефіцієнт α, що набуває значень в діапазоні $\alpha \epsilon[0,1]$, можна гнучко налаштувати важливість врахування ретроспективного усередненого показника рівня ризику, обрахованого за результатами k моделей на попередній ітерації оцінки. Цей критерій може як повністю ігноруватись, так і вносити рівноцінний вклад до поточного результуючого значення оцінки моделей, таким чином збалансовуючи і зрівноважуючи результат та згладжуючи різкі динамічні зміни результатів оцінки моделей.

Другий аргумент запропонованого методу трансформації якісної шкали оцінювання ризику в кількісний показник безпосередньо враховує критичність та число ідентифікованих вразливостей для кожного об'єкту відповідно до їх CVSS score відкритої системи класифікації та ранжування вразливостей Common Vulnerability Scoring System (CVSS). Обрахунок усередненого значення цього показника можна вдосконалити на основі середнього зваженого значення.

Зважене середнє — це статистична міра, яка враховує різну важливість (вагу) кожного елемента в наборі даних (вразливостей). Формула для обчислення зваженого середнього виглядає так:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i * w_i}{\sum_{i=1}^{n} w_i}, \quad (10)$$

де x_i — значення елемента;

w_i— відповідна вага цього елемента.

У випадку зваженого середнього з квадратичними вагами, ваги w_i визначаються як квадрати деяких величин, що відображають важливість або надійність відповідних значень x_i. Це означає, що ваги обчислюються як $w_i = {v_i}^2$, де v_i — початкова вага або міра важливості елемента.

Таким чином, формула зваженого середнього з квадратичними вагами набуває вигляду:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i * {v_i}^2}{\sum_{i=1}^{n} {v_i}^2}, \tag{11}$$

Цей підхід дозволяє надавати більшої ваги елементам з вищими значеннями, що може бути корисним у випадках, коли важливість елементів зростає нелінійно.

Якщо розглянемо випадок де $w_i = x_i$, то середнє зважене набуватиме вигляду:

$$\bar{x} = \frac{\sum_{i=1}^{n} {x_i}^2}{\sum_{i=1}^{n} x_i}, \tag{12}$$

CVSS score вже розраховується як числова оцінка рівня критичності вразливості. Використання CVSS як ваги дозволяє автоматично враховувати серйозність кожної вразливості без необхідності додаткового масштабування. Вищий CVSS означає більшу критичність вразливості, тому її вплив на загальний рівень ризику має бути більшим.

Приклад: Якщо є дві вразливості — одна з CVSS = 9.0, інша з CVSS = 4.0, то їх відносний вплив на ризик повинен бути пропорційним, що і забезпечує використання CVSS як ваги.

Якщо всі ваги рівні, то середнє зважене збігається з середнім арифметичним

$$\bar{x} = \frac{\sum_{i=1}^{n} k * x_i}{k * n} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{13}$$

де x_i — значення елемента;

k — вага елемента;

n — кількість значень.

Ваговий коефіцієнт рівня критичності активу W_i визначається на основі профілювання активів за типами та ранжування їх за важливістю для бізнес-процесів відносно шкали $W \epsilon [1,4]$. Відповідно до запропонованого підходу він може набувати значень наведених в Табл. 1.

Таблиця 1

Профілювання ІТ-активів за типами

Рівень критичності	W_i	*Приклад*
Низький	1	Пристрої системи корпоративного відеонагляду та IP-телефонії, принтери / сканери / багатофункціональні пристрої / IOT тощо
Середній	2	Мережеве обладнання, робочі станції / персональні комп'ютери, ноутбуки, планшети, тонкі клієнти тощо
Високий	3	Сервери
Критичний	4	Касові апарати, платіжні термінали, реєстратори розрахункових операцій тощо

Такий підхід дозволяє врахувати потенційні наслідки та критичність настання інцидентів ІБ відносно категорії активу та ступеню його пріоритетності для інфраструктури.

Коефіцієнт β призначений для адаптивного та гнучкого корегування показника ризику для конкретного об'єкту у разі необхідності. Враховуючи наявність механізму врахування ретроспективних показників по активу це може бути корисним в умовах практичної експлуатації в корпоративних системах.

Таким чином, можна фіналізувати математичне представлення запропонованого методу із врахуванням всіх вищеописаних рекомендацій.

$$R_{Scaled} = \mu \cdot \frac{\frac{1}{K}\sum_{i=1}^{K} \sigma_i \cdot R_i(t) + \alpha \cdot R_{old}}{1+\alpha} \cdot \frac{\sum_{j=1}^{N} CVSS_j{}^2}{2 \cdot \sum_{j=1}^{N} CVSS_j} \cdot W_i + \beta \quad , \tag{14}$$

де μ — коефіцієнт встановлення шкали оцінювання;

Основні аргументи запропонованого методу вносять рівнозважений вклад в кінцевий показник ризику. Оцінивши їх порогові значення можна констатувати, що запропонований підхід за замовчуванням надає 100-бальну шкалу оцінки ризиків ІБ, проте вона може бути гнучко налаштована за допомогою коефіцієнту μ відповідно до пріоритетів та потреб ризик-менеджменту.

Таким чином, описаний підхід дозволяє комплексно та методологічно обгрунтовано оцінити ризики кібербезпеки у розподілених системах на основі врахування результатів комплексу моделей оцінки та ряду безпекових показників, при цьому забезпечуючи гнучкість та адаптивність налаштування, оперативність аналізу та можливість легкої практичної імплементації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розглянуто проблеми і задачі формування вимог до забезпечення комплексного підходу до оцінки ризиків ІБ розподіленого середовища, а також побудови адаптивного методу кількісного оцінювання кіберризиків в РІС, що є актуальним з точки зору забезпечення ефективності застосування в динамічних умовах складних багатокомпонентних та масштабованих розподілених інформаційних систем.

Розроблений метод, інтегруючи метрико-орієнтовний підхід, може бути рекомендований для використання в сучасних РІС для комплексного аналізу ризиків ІБ, а також для оцінки ефективності системи захисту інформації. Результати дослідження можуть бути використані для побудови прикладних програмних модулів або сервісів підтримки прийняття рішень (СППР), що автоматично формують інтегральні показники ризику, виявляють закономірності та аномалії в даних і пропонують рекомендації з оптимального впровадження захисних заходів. Це сприяє покращенню якості, швидкості та прозорості процесів управління безпекою.

Запропонований підхід надає можливість створити масштабовану, адаптивну та динамічну систему управління кібер-ризиками, що ефективно реагує на сучасні загрози в РІС та значно перевершує традиційні методи аналізу ризиків. Окрім того, дозволяє оцінити ефективність та вплив впроваджених рекомендацій та заходів безпеки, і відкриває можливості для комплексного впровадження інтелектуальних систем управління інформаційною безпекою.

Напрямками подальших досліджень є розробка та підвищення ефективності комплексу моделей оцінки, заснованих на метрико-орієнтованому підході на основі інтелектуального аналізу великих обсягів гетерогенних параметрів про стан інфраструктури РІС, з метою подальшої інтеграції та застосування в рамках описаного методу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: Principles and paradigms* (2nd ed.). Prentice Hall of India.
2. Zaslavskyi, V. (2017). System principles, mathematical models and methods to ensure high reliability of safety systems. *Proceedings of SPIE*, *10418*, 1041803.
3. Norkin, V. I., Gaivoronski, A. A., Zaslavsky, V. A., & Knopov, P. S. (2018). Models of the optimal resource allocation for the critical infrastructure protection. *Cybernetics and Systems Analysis, 54*, 696–706.
4. Henry, K. (2017). Risk management and analysis. In H. F. Tipton & M. Krauze (Eds.), *Information security management handbook* (6th ed., Part 1, Section 1.4, Ch. 28, pp. 321-329). Auerbach Publications.
5. Palko, D., Vialkova, V., & Babenko, T. (2019). Intellectual models for cyber security risk assessment. In *Processing, transmission and security of information: Monografia* (Vol. 2, pp. 284–288). Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej.
6. Korchenko, A. G., Arkhipov, A. E., & Kazmirchuk, S. V. (2013). *Analysis and assessment of information security risks*. Lazurit-Poligraf.
7. Rot, A. (2008). IT risk assessment: Quantitative and qualitative approach. In *Proceedings of the World Congress on Engineering and Computer Science* (pp. 1073–1078).
8. Russell, S., & Norvig, P. (2005). *Artificial intelligence: A modern approach*. Williams.
9. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30 Rev A). National Institute of Standards and Technology.
10. FIRST. (2021). *Common Vulnerability Scoring System (CVSS) v3.1. Official Documentation.*
11. Aksu, M. U., Dilek, M. H., Tatlı, E. İ., Bicakci, K., Dirik, H. I., Demirezen, M. U., & Aykır, T. (2017, October). A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In *2017 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-8). IEEE.
12. Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*, 101659.
13. Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: The Monte Carlo predictive modelling approach. *International Journal of Critical Infrastructures, 13*(2-3), 152–167.
14. Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security, 74*, 323–339.
15. Krundyshev, V. (2020). Neural network approach to assessing cybersecurity risks in large-scale dynamic networks. In *13th International Conference on Security of Information and Networks*.
16. Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security, 22*(6), 1713–1729.
17. Gartner Report. (2023). *The role of SIEM and SOAR in modern cybersecurity strategies.* Gartner Security Insights.
18. Cebula, J. J., & Young, L. R. (n.d.). *A taxonomy of operational cyber security risks.* Carnegie Mellon University.
19. Novykov, A. N., Rodyonov, A. N., & Tymoshenko, A. A. (2015). *Models and methods of cybernetic protection of information and communication systems based on the logical-probabilistic approach: Monograph*. NTUU KPI.

20. Palko, D., Hnatienko, H., & Babenko, T. (2021, September 28–30). Determining key risks for modern distributed information systems. In *IntSol-2021 Intelligent Solutions*, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
21. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences, 13*(4), 2393. https://doi.org/10.3390/app13042393
22. Palko, D., Babenko, T., Myrutenko, L., & Bigdan, A. (2020). Model of information security critical incident risk assessment. In *Proceedings of the 2020 IEEE International Conference «Problems of Infocommunications».*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Dmytro Palko
Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-2886-1975
palko.dmytro@gmail.com

Larysa Myrutenko
Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0003-1686-261X
myrutenko.lara@gmail.com

METHOD OF COMPREHENSIVE CYBERSECURITY RISKS ASSESSMENT IN DISTRIBUTED INFORMATION SYSTEMS

Abstract. Cybersecurity risk assessment and analysis is an important element for building an effective information security management system. The high complexity and scalability of the architecture of modern distributed systems, the heterogeneity of equipment and infrastructure, as well as constant changes in the configuration and scaling of the environment give rise to a number of problems related to the collection and analysis of information for risk assessment, the need for operational processing of large arrays of complex in structure and heterogeneous in nature data coming from differentiated security and monitoring systems, event logs, audit reports and other sources, as well as the lack of a single format for their presentation. The limitations of existing standards and methodologies in the dynamic conditions of modern DIS, their conceptual nature and the complexity of practical implementation and application require the development of flexible methodological and technological solutions for cyber risk analysis that would integrate the advantages of existing approaches, provide automation of calculations and take into account the dynamic aspects of distributed environment. The article presents a comprehensive adaptive method for quantitative assessment of cybersecurity risks in distributed information systems, which is relevant in dynamic conditions of complex multi-component and scalable DIS. The proposed method, integrating a metric-oriented approach based on the results of a complex of neural network models for assessing DIS infrastructure security indicators and compliance metrics for regulatory frameworks and leading standards, provides an opportunity to create a scalable and dynamic cyber risk management system that effectively responds to modern threats in DIS and open opportunities for the comprehensive implementation of intelligent information security management systems in risk management processes.

Keywords: cybersecurity; information security; information security risk; risk assessment; risk management; distributed information system; neural network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: Principles and paradigms* (2nd ed.). Prentice Hall of India.
2. Zaslavskyi, V. (2017). System principles, mathematical models and methods to ensure high reliability of safety systems. *Proceedings of SPIE*, *10418*, 1041803.
3. Norkin, V. I., Gaivoronski, A. A., Zaslavsky, V. A., & Knopov, P. S. (2018). Models of the optimal resource allocation for the critical infrastructure protection. *Cybernetics and Systems Analysis, 54*, 696–706.
4. Henry, K. (2017). Risk management and analysis. In H. F. Tipton & M. Krauze (Eds.), *Information security management handbook* (6th ed., Part 1, Section 1.4, Ch. 28, pp. 321-329). Auerbach Publications.

5. Palko, D., Vialkova, V., & Babenko, T. (2019). Intellectual models for cyber security risk assessment. In *Processing, transmission and security of information: Monografia* (Vol. 2, pp. 284–288). Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej.
6. Korchenko, A. G., Arkhipov, A. E., & Kazmirchuk, S. V. (2013). *Analysis and assessment of information security risks*. Lazurit-Poligraf.
7. Rot, A. (2008). IT risk assessment: Quantitative and qualitative approach. In *Proceedings of the World Congress on Engineering and Computer Science* (pp. 1073–1078).
8. Russell, S., & Norvig, P. (2005). *Artificial intelligence: A modern approach*. Williams.
9. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30 Rev A). National Institute of Standards and Technology.
10. FIRST. (2021). *Common Vulnerability Scoring System (CVSS) v3.1. Official Documentation.*
11. Aksu, M. U., Dilek, M. H., Tatlı, E. İ., Bicakci, K., Dirik, H. I., Demirezen, M. U., & Aykır, T. (2017, October). A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In *2017 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-8). IEEE.
12. Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*, 101659.
13. Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: The Monte Carlo predictive modelling approach. *International Journal of Critical Infrastructures, 13*(2-3), 152–167.
14. Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security, 74*, 323–339.
15. Krundyshev, V. (2020). Neural network approach to assessing cybersecurity risks in large-scale dynamic networks. In *13th International Conference on Security of Information and Networks*.
16. Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security, 22*(6), 1713–1729.
17. Gartner Report. (2023). *The role of SIEM and SOAR in modern cybersecurity strategies.* Gartner Security Insights.
18. Cebula, J. J., & Young, L. R. (n.d.). *A taxonomy of operational cyber security risks.* Carnegie Mellon University.
19. Novykov, A. N., Rodyonov, A. N., & Tymoshenko, A. A. (2015). *Models and methods of cybernetic protection of information and communication systems based on the logical-probabilistic approach: Monograph*. NTUU KPI.
20. Palko, D., Hnatienko, H., & Babenko, T. (2021, September 28–30). Determining key risks for modern distributed information systems. In *IntSol-2021 Intelligent Solutions*, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
21. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences, 13*(4), 2393. https://doi.org/10.3390/app13042393
22. Palko, D., Babenko, T., Myrutenko, L., & Bigdan, A. (2020). Model of information security critical incident risk assessment. In *Proceedings of the 2020 IEEE International Conference «Problems of Infocommunications».*