КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.845
УДК 004.056.55

Абрамов Вадим Олексійович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-8026-1475
v.abramov@kubg.edu.ua

Глушак Оксана Михайлівна
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-9849-1140
o.hlushak@kubg.edu.ua

Плоха Ангеліна Юріївна
студентка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0003-5327-999X
ayplokha.fitu21@kubg.edu.ua

Довженко Тимур Павлович
кандидат технічнихнаук, доцент, доцент кафедри інженерії програмного забезпечення
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0006-9930-5091
timurdov@ukr.net

ПРОЄКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ВИМОГ КІБЕРБЕЗПЕКИ: ПІДХОДИ ТА РЕАЛІЗАЦІЯ НА БАЗІ CISCO

Анотація. У статті здійснено комплексне дослідження сучасних підходів до проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки, з акцентом на практичну реалізацію за допомогою технологій Cisco. В умовах зростання цифрових загроз та ускладнення інформаційних систем особливого значення набуває інтеграція механізмів захисту ще на ранніх етапах проєктування. Розглянуто концепції Security-by-Design, архітектури Zero Trust, мікросегментації та використання цифрових двійників для імітаційного тестування. Показано, що впровадження принципу «ніколи не довіряй, завжди перевіряй» дозволяє локалізувати інциденти безпеки, зменшити ризики горизонтального поширення атак та забезпечити постійний контроль за доступом. Значну увагу приділено побудові багаторівневої мережевої архітектури із застосуванням VLAN, ACL, WPA3, Port Security та локальної аутентифікації. У середовищі Cisco Packet Tracer змодельовано зіркоподібну мережу з дев'ятьма логічними сегментами, що обслуговує до 300 користувачів із високими вимогами до пропускної здатності, стабільності з'єднання та захисту даних. Запропоновано сценарії фільтрації вхідного трафіку, захисту бездротових точок доступу, а також організації резервного копіювання із захистом переданих даних через FTP з автентифікацією. Результати підтверджують доцільність застосування комплексного підходу, що забезпечує відповідність чинним стандартам захисту інформації. Перспективи подальших досліджень пов'язані з адаптацією описаних методик для галузей із підвищеними вимогами до кібербезпеки.

Ключові слова: мережева інфраструктура; кібербезпека; проєктування мереж; Cisco; інформаційна безпека.

ВСТУП

У сучасному цифровому світі безпека мережевої інфраструктури стала критичним фактором для забезпечення стабільної роботи організацій будь-якого масштабу. Зростання кількості та складності кібератак, збільшення поверхні атаки через розширення мережевої інфраструктури та впровадження нових технологій вимагають комплексного підходу до проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки [1]. Сучасні кіберзлочинці постійно вдосконалюють свої методи атак, використовуючи все більш складні та цілеспрямовані підходи. Україна, за даними експертів з кібербезпеки, ще до початку повномасштабної війни була серед країн з високим рівнем кіберзагроз. Протягом 2022 року урядова команда CERT-UA зафіксувала понад дві тисячі кібератак, що свідчить про надзвичайно високий рівень активності в цій сфері [2]. З початком повномасштабної війни кількість кібератак проти України продовжувала зростати. У 2023 році кількість зафіксованих кібератак збільшилася на 15,9% порівняно з 2022 роком, сягнувши 2,543 випадків [3]. Найбільш драматичне зростання спостерігалося у 2024 році: кількість кібератак зросла майже на 70%, досягнувши 4,315 інцидентів порівняно з 2,541 у 2023 році [4]. Така динаміка кіберінцидентів підкреслює нагальну потребу в розробці комплексних підходів до створення захищеної мережевої інфраструктури.

Постановка проблеми. У сучасних умовах цифровізації та стрімкого розвитку інформаційних технологій питання проєктування надійної, масштабованої та безпечної мережевої інфраструктури набуває особливої актуальності. Зростання обсягів даних, поширення хмарних сервісів, віддаленого доступу та Інтернету речей (IoT) висуває нові вимоги до проєктування мереж, які повинні не лише забезпечувати ефективну комунікацію, а й бути стійкими до кіберзагроз.

Однією з основних проблем є недостатня інтеграція механізмів кібербезпеки на етапі проєктування мережевої інфраструктури. У багатьох випадках заходи безпеки впроваджуються постфактум, що знижує загальну стійкість системи до атак, створює вразливості та ускладнює адміністрування. Крім того, відсутність єдиного підходу до побудови безпечних мереж у різних організаціях призводить до фрагментарності рішень і зниження ефективності їх захисту.

Сучасні технології компанії Cisco надають широкий спектр інструментів для побудови як інфраструктури, так і системи кіберзахисту, проте ефективне використання цих технологій потребує комплексного підходу, що враховує вимоги до безпеки вже на початковому етапі проєктування. Таким чином, виникає потреба у дослідженні методичних і технологічних засад побудови мережевої інфраструктури з урахуванням принципів кібербезпеки, а також у розробці практичних рішень, реалізованих на базі обладнання та програмних засобів Cisco.

Це визначає актуальність теми та обумовлює необхідність створення цілісної моделі безпечної мережевої інфраструктури з урахуванням сучасних загроз і можливостей, що забезпечуються інструментами Cisco.

Аналіз останніх досліджень і публікацій. Огляд наукових публікацій, присвячених проєктуванню мережевої інфраструктури з урахуванням вимог кібербезпеки, дає підстави для систематизації досліджуваного матеріалу за трьома ключовими напрямами. Перший напрям — архітектурне проєктування з вбудованою безпекою — охоплює концепції та підходи, які передбачають інтеграцію засобів захисту ще на етапі формування архітектури мережевих систем. Другий напрям — інноваційні технології та інтелектуальні підходи до захисту — включає сучасні методи на основі

штучного інтелекту, цифрових двійників, програмно-визначених мереж і архітектури нульової довіри, які забезпечують адаптивну та проактивну безпеку. Третій напрям — регуляторні, правові та міждисциплінарні аспекти кібербезпеки — зосереджений на нормативно-правовому забезпеченні, кадровій підготовці, міжгалузевій взаємодії та організаційних викликах, які впливають на ефективність побудови та функціонування захищеної мережевої інфраструктури. Такий поділ дозволяє здійснити комплексний аналіз теми та виявити стратегічні напрями її розвитку.

Сучасні тенденції в мережевій інженерії дедалі частіше орієнтуються на принципи безпеки на етапі проєктування (security by design), що передбачає інтеграцію механізмів захисту на всіх рівнях архітектури ще до впровадження системи. Дослідження [5] підкреслює необхідність поєднання практик кібербезпеки з мережею через впровадження таких стратегій, як Zero Trust, мікросегментація, DevSecOps та програмно-визначені мережі (SDN). Подібно, [6] звертає увагу на важливість моделювання загроз як складової проєктування, наголошуючи на потенціалі автоматизованих підходів до передбачення вразливостей. [7] і [8] акцентують на потребі глибокої попередньої оцінки безпеки в системах IoT, застосовуючи архітектури з поділом на логічні домени, які легко адаптуються до вимог критичної інфраструктури. Архітектурні моделі цифрових двійників, як у [9] та [10], також розглядаються як інструмент інтегрованого підходу до безпеки, дозволяючи ще на етапі моделювання виявляти критичні точки атаки та формувати ефективні контрзаходи. Така системна інтеграція безпеки не лише знижує витрати на усунення загроз, а й підвищує стійкість систем до зовнішніх впливів.

Другий напрям фокусується на застосуванні новітніх технологій — насамперед, цифрових двійників, штучного інтелекту, графових нейромереж та архітектур Zero Trust — для створення адаптивних, гнучких і самооновлюваних систем безпеки. Так, [11] пропонує автономну довірену мережу (ATN), що використовує цифрові двійники та AI для проактивного виявлення загроз і динамічного налаштування політик. [12] демонструє ефективність цифрових двійників у критичній інфраструктурі як елементу проєктування кіберфізичних систем. Архітектура нульової довіри, всебічно розглянута в роботах [13] – [16], виступає сучасною моделлю організації мережевого доступу, де автентифікація, авторизація і мікросегментація є основними механізмами забезпечення цілісності системи. Додатково, [17] демонструє приклад ефективного використання машинного навчання у реальному середовищі малого підприємства для виявлення атак нульового дня, порівнюючи open-source і комерційні інструменти. Застосування цих підходів дозволяє забезпечити не лише миттєву реакцію на загрози, а й формування безпекових стратегій на основі аналітики, поведінкових патернів і моделювання сценаріїв.

Третій напрям охоплює питання правового регулювання, політики захисту даних, а також людського та організаційного факторів у контексті мережевої безпеки. В роботі [2] проаналізовано стан нормативно-правової бази України в галузі кібербезпеки, її відповідність міжнародним вимогам, а також потенціал використання штучного інтелекту у державній системі захисту. Актуальним є також питання міждисциплінарної підготовки кадрів, на якому акцентують [5] і [7], підкреслюючи потребу в універсальних фахівцях, здатних працювати на стику інженерії, безпеки, управління й аналітики. У свою чергу, [17] демонструє, як в умовах обмежених ресурсів малого бізнесу впровадження технічних рішень часто стикається з кадровими та економічними бар’єрами, що також повинні враховуватися при плануванні безпечної інфраструктури. Регуляторні аспекти, стандарти захисту даних (як-от GDPR), а також організаційні протоколи стають критично важливими для інтеграції технічних рішень у реальні системи з урахуванням економіки, культури та інституційного контексту.

Узагальнюючи результати огляду, можна констатувати, що ефективне проєктування мережевої інфраструктури в умовах зростаючих кіберзагроз вимагає системного підходу, який поєднує архітектурні принципи безпеки, інноваційні технології захисту та дотримання нормативно-правових вимог. Інтеграція кібербезпеки на всіх етапах проєктування, впровадження інтелектуальних систем виявлення загроз, а також урахування організаційних і правових чинників формують основу для побудови надійних і стійких мережевих рішень. У цьому контексті особливу увагу заслуговують практичні приклади реалізації зазначених підходів, які демонструють їхню ефективність у реальному корпоративному середовищі.

Мета статті. Метою статті є обґрунтування сучасних підходів до проєктування мережевої інфраструктури з урахуванням актуальних вимог кібербезпеки, а також аналіз особливостей їх реалізації на прикладі рішень Cisco з метою підвищення надійності, стійкості та захищеності корпоративних мереж.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні підходи поєднують інтеграцію безпеки на всіх етапах проєктування, використання цифрових двійників, Zero Trust, мікросегментацію та машинне навчання для підвищення стійкості мережі до кіберзагроз.

Основні підходи до проєктування безпечної мережі

Security-by-Design: Впровадження принципів безпеки на ранніх етапах проєктування мережі дозволяє мінімізувати вразливості та забезпечити стійкість до сучасних атак. Важливо інтегрувати кібербезпеку у всі рівні архітектури, а не додавати її постфактум [5].

Zero Trust та мікросегментація: Використання Zero Trust-архітектури та мікросегментації дозволяє ізолювати сегменти мережі, обмежуючи розповсюдження атак та підвищуючи контроль доступу [5], [8].

Цифрові двійники: Створення цифрових двійників мережевої інфраструктури дає змогу моделювати атаки, тестувати контрзаходи та оптимізувати захист без впливу на реальні системи [10], [12].

Розглянемо більш детально кожен з підходів.

Підхід Security-by-Design (безпека за задумом) передбачає інтеграцію вимог безпеки на всіх етапах життєвого циклу проєктування мережевої інфраструктури, починаючи з фази ініціалізації та моделювання. Його основною концепцією є запобігання загрозам шляхом врахування аспектів кібербезпеки з самого початку, що дозволяє значно зменшити ризики, підвищити стійкість системи до атак та забезпечити відповідність сучасним стандартам безпеки.

Одним із ключових принципів даного підходу є вбудована безпека на етапі проєктування, що передбачає одночасне визначення функціональних і захисних вимог ще на початковій стадії проєкту. Використовуються спеціалізовані методології для аналізу потенційних загроз, моделювання можливих векторів атак та впровадження механізмів протидії ще до етапу реалізації системи [6], [7].

Моделювання загроз і оцінка ризиків становлять центральний компонент Security-by-Design. Систематичне виявлення вразливостей, визначення критичних точок входу для потенційних атак, а також використання автоматизованих інструментів для threat modeling дозволяють зменшити імовірність виникнення інцидентів та оптимізувати витрати на забезпечення кібербезпеки [6], [7].

Значну роль відіграє мікросегментація мережі, яка полягає у логічному поділі інфраструктури на ізольовані сегменти з метою локалізації впливу потенційних атак. Доповненням до цього є реалізація принципу найменших привілеїв, згідно з яким користувачам і сервісам надається лише той рівень доступу, який є необхідним для виконання їхніх функцій [18].

Інтеграція сучасних технологій забезпечує реалізацію високого рівня безпеки в динамічному цифровому середовищі. Серед таких технологій — криптографічний захист даних, адаптивна автентифікація, використання технологій блокчейну для забезпечення цілісності та конфіденційності, а також впровадження багаторівневої (layered) архітектури безпеки, що забезпечує модульність і гнучкість у реагуванні на нові загрози [19].

Таким чином, реалізація принципів Security-by-Design сприяє створенню надійної, масштабованої та стійкої до атак мережевої інфраструктури, що відповідає вимогам сучасного кіберзахисту.

Сегментація ділить мережу на менші підмережі, що спрощує управління трафіком і обмежує розповсюдження атак. Зазвичай виділяють такі зони: зовнішня (Інтернет), DMZ (демілітаризована зона з публічними сервісами), внутрішня корпоративна мережа (LAN), гостьова та IoT-зона. Для кожної зони застосовують окремі правила безпеки (настроювані міжзональні фаєрволи, маршрутизатори з ACL, VLAN ACL тощо) [20].

Такий підхід є складовою «Defense in Depth» — багаторівневої оборони, коли шари захисту (фізичні, мережеві, прикладні) накладаються один на один. За визначенням NIST, Defense-in-Depth — це інформаційна стратегія, що інтегрує людей, технології та операції для створення багаторівневих бар'єрів захисту [21]. В контексті мережевої безпеки реалізуються й концепції Zero Trust. За ними жоден сегмент мережі не вважається «довіреним» за замовчуванням: кожне з'єднання і запит перевіряється в реальному часі. Так, Zero Trust-модель передбачає постійне підтвердження автентичності користувачів і пристроїв перед наданням доступу. Зокрема, її архітектура передбачає поділ безпеки на три ключові напрями, кожен з яких має комплексний підхід до захисту цифрової інфраструктури.

Перший напрям — безпека користувачів і пристроїв — передбачає постійну автентифікацію та перевірку кожного користувача й кожного пристрою незалежно від їхнього фізичного чи мережевого розташування. Застосовується багатофакторна автентифікація, аналіз поведінки, оцінка стану пристрою, а також реалізується принцип найменших привілеїв — доступ дозволяється виключно до тих ресурсів, які дійсно необхідні [13], [16].

Другий напрям — мережева та хмарна безпека — ґрунтується на мікросегментації мережі, що дозволяє обмежити горизонтальне переміщення потенційних загроз усередині інфраструктури. Впроваджується безперервний моніторинг трафіку, автоматизоване виявлення аномалій і швидке реагування на інциденти. Модель Zero Trust також ефективно адаптується до хмарних і гібридних середовищ, ураховуючи їхню динамічну природу [14], [15].

Третій напрям — безпека додатків і даних — забезпечується завдяки ретельному контролю доступу, який базується на ідентичності користувача, контексті взаємодії та політиках безпеки. Дані захищаються за допомогою шифрування, проводиться аудит доступу та впроваджуються заходи для запобігання несанкціонованому використанню інформації [13], [16].

Завдяки комплексному охопленню, модель Cisco Zero Trust формує гнучке й надійне середовище, де довіра не є за замовчуванням, а безпека — це не стіна, а постійно

діючий процес перевірки, моніторингу та адаптації. Наприклад, усі корпоративні дані та сервіси вважаються «зовнішніми», і доступ до них надається за принципом найменшого привілея та з динамічним моніторингом. У сукупності застосування сегментації, Defense-in-Depth та Zero Trust дозволяє мінімізувати розповсюдження загрози й забезпечити комплексний захист мережі.

Цифрові двійники набувають усе більшого значення як інструмент для проєктування безпечних мереж в умовах зростаючої складності інфраструктури та підвищених вимог до захисту даних. Віртуальні копії фізичних систем дозволяють здійснювати моделювання, моніторинг, тестування та впровадження стратегій безпеки ще до появи реальних загроз, що відкриває нові можливості для підвищення стійкості мереж до зовнішніх і внутрішніх атак.

Одним із перспективних напрямів є створення автономних довірених мереж [11], у яких цифрові двійники використовуються для збору телеметричних даних, навчання моделей безпеки із застосуванням графових нейронних мереж та автоматичного формування політик захисту. Такий підхід забезпечує проактивне виявлення загроз та швидке реагування на них, що суттєво перевершує ефективність традиційних методів фільтрації чи маршрутизації трафіку. У промислових системах синхронізація станів між фізичними та цифровими компонентами забезпечує безпечне оновлення програмного забезпечення та контроль критичних технологічних процесів, що особливо актуально в умовах безперервного виробничого циклу [9].

Цифрові двійники відкривають нові можливості для проєктування безпечних мереж завдяки моделюванню, проактивному виявленню загроз, використанню сучасних криптографічних рішень та інтеграції блокчейну й AI. Вони дозволяють виявляти вразливості на ранніх етапах, забезпечують гнучкість і масштабованість захисту, а також підвищують довіру до мережевих систем.

Cisco-технології дають змогу реалізувати політики безпеки, сегментації, моніторингу та реагування на інциденти (табл. 1) [17].

Таблиця 1

Технологічна реалізація на базі Cisco

Технологія Cisco	Призначення
Cisco ASA/Firepower	Міжмережеві екрани, IDS/IPS
Cisco SDN	Гнучке управління політиками безпеки
Cisco ISE	Контроль доступу, ідентифікація користувачів
Cisco Umbrella	Захист DNS, хмарна безпека
Cisco Meraki	Хмарне управління мережами

Далі розглянемо приклад практичної реалізації мережевої інфраструктури з урахуванням вимог до безпеки на базі рішень Cisco та основних підходів до проєктування безпечної мережі, що дозволяє наочно проілюструвати застосування теоретичних аспектів на практиці.

З метою конкретизації розглянемо типовий сценарій побудови корпоративної мережі, що враховує актуальні вимоги до безпеки, масштабованості та продуктивності. Такий приклад дозволяє перейти від загальних принципів до аналізу технічних рішень і параметрів, необхідних для реалізації ефективної мережевої інфраструктури.

Розробка топології для мережі вимагає ґрунтовного аналізу вимог, які забезпечать її ефективність, адаптивність і відповідність сучасним стандартам. Мережа планується для обслуговування до 200-300 користувачів. Однією з ключових потреб є висока пропускна спроможність, яка дозволить підтримувати інтенсивне використання

цифрових платформ, таких як відеозв'язок і хмарні сервіси. З огляду на можливу кількість одночасних з'єднань (до 300 пристроїв — комп'ютерів, планшетів і ноутбуків), мінімальна швидкість зв'язку з зовнішніми ресурсами має сягати 1 Гбіт/с, а локальні сегменти — бути готовими до обробки мультимедійного контенту, включаючи потокове відео. Точки доступу Wi-Fi повинні забезпечувати стабільне покриття в кожній зоні з можливістю підключення до 50 користувачів із пропускною спроможністю до 1,7 Гбіт/с.

Логічна схема побудована на зіркоподібному принципі, де головний маршрутизатор є центральним елементом, що об'єднує всі зони через механізм міжмережевого обміну VLAN. Мережа поділена на дев'ять підмереж, відповідно до підходу мікросегментації, що дозволяє розмежувати потоки даних між різними групами користувачів і серверами, забезпечуючи зручне адміністрування та захист.

Застосування підходу мікросегментації дозволяє логічно структурувати мережу, що забезпечує ефективне розмежування трафіку та ізоляцію сегментів для підвищення рівня безпеки. Головний маршрутизатор забезпечуватиме обмін даними між цими сегментами, дозволяючи, наприклад, користувачам із VLAN 10 звертатися до серверів у VLAN 40, але блокуючи їхній доступ до VLAN 30, що підвищить захист.

Захист мережі планується організувати на кількох рівнях. Для бездротового зв'язку в трьох зонах буде використано шифрування WPA3, щоб запобігти несанкціонованому підключенню. Автентифікація користувачів здійснюватиметься через систему RADIUS, розміщену в VLAN 40, що дозволить розмежувати права доступу різних користувачів. Наприклад, користувачі з VLAN 10 і 20 не зможуть підключатися до VLAN 30, а гостьова зона (VLAN 50) буде відокремлена від решти мережі.

Головний маршрутизатор матиме вбудовані механізми захисту від зовнішніх атак, таких як DDoS, і контролюватиме потоки даних між сегментами.

Головний маршрутизатор відповідатиме за передачу даних між VLAN, забезпечуючи зв'язок між зонами. Наприклад, пристрої з VLAN 10 зможуть звертатися до серверів у VLAN 40. Для забезпечення пріоритету важливого трафіку, наприклад, для відеозв'язку, планується впровадження QoS, що мінімізує затримки. Зовнішній зв'язок зі швидкістю 1 Гбіт/с гарантуватиме достатню пропускну здатність для всіх користувачів, включаючи доступ до хмарних платформ і потокового контенту.

Логічна схема передбачає можливість розширення: нові зони чи пристрої можна буде додавати без значних змін у структурі. У кожній зоні передбачається розміщення принтерів, доступних для відповідних груп, а сервери у VLAN 40 забезпечуватимуть збереження даних для захисту документів.

У програмному середовищі Cisco Packet Tracer було розроблено модель мережевої архітектури, яка являє собою реалізацію зіркоподібної топології, створеної на основі попередньо визначеної логічної моделі (рис.1).

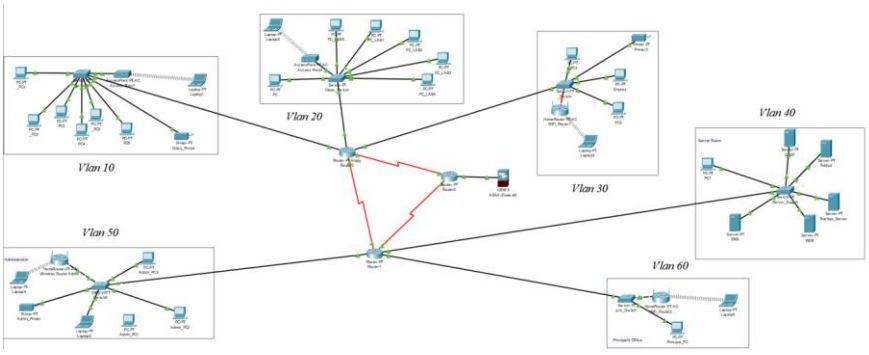

Рис. 1. Топологія мережі у Cisco Packet Tracer

Для кожного пристрою вказано IP-адресу, маску підмережі та шлюз за замовчуванням, що відповідає підмережі конкретної VLAN. Особливу увагу приділено тому, щоб шлюз для кожного пристрою відповідав IP-адресі підключеного інтерфейсу маршрутизатора у відповідній VLAN.

Реалізовано фільтрацію вхідного трафіку за допомогою списку контролю доступу (ACL), застосованого на зовнішньому інтерфейсі маршрутизатора Router0. Це дозволило обмежити вхідні з'єднання з боку зовнішньої мережі, зокрема блокувати ICMP-запити.

На маршрутизаторі Router2 створено та застосовано список контролю доступу з назвою VLAN_ISOLATION, який блокує доступ з підмереж VLAN10 і VLAN20 до підмережі VLAN30. Це досягається шляхом заборони ICMP-пакетів у відповідному напрямку.

На комутаторах увімкнено Port Security, який обмежує підключення до одного пристрою на порт із фіксацією MAC-адреси в режимі Sticky. Це блокує спроби підключення неавторизованих пристроїв, наприклад, особистих ноутбуків, що не належать до адміністративної інфраструктури. Виявлення порушень призводить до автоматичного блокування порту, що захищає чутливі дані, такі як фінансові звіти чи персональна інформація працівників.

На прикладі інтерфейсу FastEthernet3/1 наведено параметри активного контролю доступу (рис. 2).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#do show port-security int fa3/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.2F41.8003:50
Security Violation Count   : 1
```

Рис.2. Port-security інтерфейсу FastEthernet3/1

Функція безпеки ввімкнена (Port Security: Enabled), порт перебуває в стані Secure-up, що вказує на відсутність порушень під час роботи. Встановлено обмеження на підключення лише одного пристрою до кожного порту (Maximum MAC Addresses: 1), а динамічно вивчена MAC-адреса збережена в режимі Sticky.

Зафіксовано один випадок порушення (Security Violation Count: 1), який виник внаслідок спроби підключити інший пристрій, що було заблоковано відповідно до політики контролю.

Базове обмеження доступу реалізовано на маршрутизаторі Router1 шляхом налаштування локальної аутентифікації та шифрування паролів. Встановлено пароль на консольний доступ, що запобігає несанкціонованому підключенню до пристрою (рис. 3). Додатково введено пароль для переходу в привілейований режим, а всі паролі зашифровано командою service password-encryption. Також додано банер із попередженням про заборону неавторизованого доступу, який відображається при спробі з'єднання.

ISSN 2663 - 4023

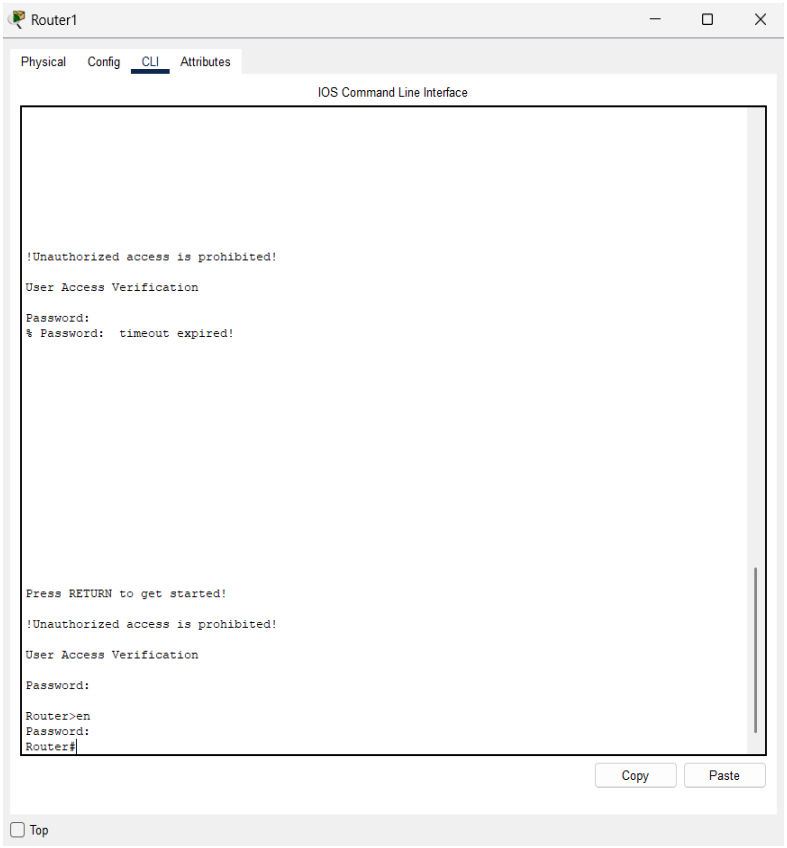

Рис.3. Базовий захист на Router1

Для захисту мережі реалізовано комплекс заходів, спрямованих на захист даних, обмеження доступу та запобігання кіберзагрозам, що відповідає потребам організації в безпечному інформаційному середовищі та стандартам щодо захисту даних. На зовнішньому маршрутизаторі Router0 застосовано фільтрацію вхідного трафіку за допомогою списків контролю доступу, які блокують спроби сканування мережі, зокрема через ICMP-протокол.

Це захищає внутрішні ресурси від розвідувальних атак, які можуть передувати складнішим кібератакам, як-от DDoS. Доступ до сервісів, таких як веб-ресурси, DNS-запити та HTTPS-з'єднання, збережено, що забезпечує безперебійну роботу платформ. Цей захід знижує ризик зовнішнього втручання, дозволяючи користувачам безпечно використовувати онлайн-ресурси.

Завдяки поділу мережі на мікросегменти у вигляді дев'яти VLAN досягається ізоляція трафіку між групами користувачів, що сприяє підвищенню рівня безпеки та контролю доступу. Це зменшує ймовірність несанкціонованого доступу до чутливих даних, таких як документація. На маршрутизаторі Router2 налаштовано правила ACL, які обмежують міжзонний трафік, зокрема забороняють зв'язок між підмережами, захищаючи інформацію. Доступ до серверної зони відкрито для всіх користувачів, щоб забезпечити використання спільних ресурсів. Сегментація підвищує безпеку, оптимізує трафік і полегшує управління мережею. Бездротовий зв'язок захищено шифруванням WPA3 на всіх точках доступу, що відповідає сучасним стандартам безпеки Wi-Fi. Це запобігає перехопленню даних і підключенню сторонніх пристроїв, що є важливим у організації, де часто використовують власні гаджети. WPA3 застосовує стійкі криптографічні алгоритми, забезпечуючи захист навіть при високому навантаженні на бездротову мережу.

Цей механізм є ефективним для запобігання несанкціонованому доступу в адміністративному блоці. Маршрутизатор Router1 захищено локальною автентифікацією з паролями для доступу до консолі та привілейованого режиму, зашифрованими командою service password-encryption. Додано банер із повідомленням про заборону несанкціонованого доступу, який відображається при спробі підключення. Ці заходи захищають керуючі елементи мережі від неавторизованого втручання, що є критично важливим для стабільної роботи інфраструктури та захисту конфігураційних налаштувань.

Автентифікацію користувачів моделює веб-інтерфейс на WEB-сервері з формою для введення логіну та пароля, що дозволяє імітувати контроль доступу до спільних ресурсів. Цей інтерфейс демонструє можливість розмежування доступу для різних груп користувачів, що сприяє захисту даних і підвищує контроль над ресурсами мережі. Резервне копіювання даних організовано через Python-скрипт, який передає файли, наприклад index.html, на FTP-сервер із автентифікацією. Це забезпечує збереження документації і конфігураційних даних у разі збоїв чи атак. Використання FTP-протоколу з автентифікацією обмежує доступ до сервера лише авторизованим користувачам, що знижує ризик втрати чи компрометації інформації. Цей механізм підтримує безперервність роботи з даними, дозволяючи швидко їх відновлювати.

Застосовані заходи відповідають стандартам щодо захисту даних, зокрема вимогам Закону України «Про захист персональних даних» [22-26], який регулює обробку персональних даних у навчальних закладах, вимагаючи захисту від несанкціонованого доступу, втрати чи модифікації.

Ці заходи забезпечують конфіденційність, цілісність та доступність даних, що є важливим для захисту інформації, а також відповідають принципам обробки даних, визначеним у Державних санітарних правилах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження було здійснено комплексний аналіз сучасних підходів до проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки та їх практичної реалізації на базі технологій Cisco.

Дослідження показало, що інтеграція принципів кібербезпеки на етапі проєктування мережевої інфраструктури є критично важливою для забезпечення надійного захисту організацій від сучасних кіберзагроз. Підхід Security-by-Design виявився найбільш ефективним для мінімізації вразливостей шляхом вбудовування механізмів безпеки з початкових етапів розробки системи, що дозволяє значно зменшити ризики та підвищити стійкість до атак.

Запропонована архітектура Zero Trust з мікросегментацією мережі демонструє високу ефективність у запобіганні горизонтальному поширенню загроз та забезпеченні детального контролю доступу. Реалізація принципу "ніколи не довіряй, завжди перевіряй" через постійну автентифікацію користувачів і пристроїв суттєво підвищує рівень захисту корпоративних мереж.

Використання цифрових двійників як інструменту моделювання та тестування стратегій безпеки відкриває нові можливості для проактивного виявлення загроз та оптимізації захисних механізмів без впливу на продуктивні системи. Це дозволяє організаціям готуватися до потенційних атак та розробляти ефективні контрзаходи.

Практична реалізація запропонованих підходів у середовищі Cisco Packet Tracer підтвердила життєздатність розробленої моделі мережевої інфраструктури для обслуговування 200-300 користувачів. Впровадження зіркоподібної топології з дев'ятьма VLAN забезпечило ефективну сегментацію трафіку та ізоляцію критичних ресурсів.

Комплекс заходів безпеки, включаючи фільтрацію трафіку через ACL, захист бездротової мережі за допомогою WPA3, Port Security на комутаторах та автентифікацію на мережевих пристроях, створив багаторівневу систему захисту, що відповідає сучасним стандартам кібербезпеки.

Перспективним напрямом подальших досліджень є вивчення особливостей проєктування безпечних мережевих інфраструктур для специфічних галузей, таких як охорона здоров'я, фінансовий сектор та об'єкти критичної інфраструктури, з урахуванням їхніх унікальних вимог до конфіденційності, доступності та цілісності даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco. (2025, June). *Cisco unveils secure network architecture to accelerate workplace AI transformation*. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m06/cisco-unveils-secure-network-architecture-to-accelerate
2. Сироватченко, М. (2024). Правові аспекти забезпечення кібербезпеки в Україні: Сучасні виклики та роль національного законодавства. *Вісник Національного університету "Львівська політехніка". Серія: Юридичні науки, 1*(41), 314–320. https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf
3. Smith, B. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Security. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war
4. Microsoft. (2022). *The hybrid war in Ukraine*. Microsoft . https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
5. Bellamkonda, S. (2023). Cybersecurity and network engineering: Bridging the gap for optimal protection. *International Journal of Innovative Research in Science, Engineering and Technology*. https://doi.org/10.15680/ijirset.2023.1204007
6. Granata, D., & Rak, M. (2023). Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. *Software Quality Journal, 32*, 125–161. https://doi.org/10.1007/s11219-023-09634-4
7. Diamantopoulou, V., & Mouratidis, H. (2018). A security analysis method for industrial internet of things. *IEEE Transactions on Industrial Informatics, 14*, 4093–4100. https://doi.org/10.1109/TII.2018.2832853
8. Colajanni, M., Zanasi, C., & Russo, S. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks, 156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414
9. Gehrmann, C., & Gunnarsson, M. (2020). A digital twin based industrial automation and control system security architecture. *IEEE Transactions on Industrial Informatics, 16*, 669–680. https://doi.org/10.1109/TII.2019.2938885
10. Masi, M., Aranha, H., Sellitto, G., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling, 22*, 689–707. https://doi.org/10.1007/s10270-022-01075-0
11. Li, L., Gao, S., Zhang, W., Wu, J., Liu, Y., Xia, Y., & Zhang, H. (2024). Toward autonomous trusted networks – From digital twin perspective. *IEEE Network, 38*, 84–91. https://doi.org/10.1109/MNET.2024.3353180
12. Bravo-Haro, M., Broo, D., & Schooling, J. (2022). Design and implementation of a smart infrastructure digital twin. *Automation in Construction*. https://doi.org/10.1016/j.autcon.2022.104171
13. Chen, L., Ni, Y., Huang, D., He, Y., & X., Y. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2022/6476274
14. Liu, J., Liu, G., Meng, L., Wang, Q., & Kang, H. (2023). Theory and application of zero trust security: A brief survey. *Entropy, 25*. https://doi.org/10.3390/e25121595
15. Sarkar, S., Choudhary, G., Hussain, A., Kim, H., & Shandilya, S. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability, 14*(18), 11213. https://doi.org/10.3390/su141811213

16. Syed, N., Anwar, A., Shah, S., Doss, R., Shaghaghi, A., & Baig, Z. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679
17. Hewage, C., Rawindaran, N., Prakash, E., & Jayal, A. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet, 13*, 186. https://doi.org/10.3390/fi13080186
18. Feng, D. (2024). The basics of creating secure data architectures for financial organizations. *The American Journal of Engineering and Technology*. https://doi.org/10.37547/tajet/volume06issue12-13
19. Aladwan, M., Alawadi, S., Awaysheh, F., Cabaleiro, J., Alazab, M., & Pena, T. (2021). Security by design for big data frameworks over cloud computing. *IEEE Transactions on Engineering Management, PP*, 1–18. https://doi.org/10.1109/TEM.2020.3045661
20. Cisco. (n.d.). *What is network segmentation?* https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html
21. National Institute of Standards and Technology. (n.d.). *Defense in depth*. https://csrc.nist.gov/glossary/term/defense_in_depth
22. Верховна Рада України. (2010). *Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010*. https://zakon.rada.gov.ua/laws/show/2297-17#Text
23. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
24. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
25. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
26. Abamov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., ... Yaskevych, V. (2021). *Theoretical and practical aspects of the use of mathematical methods and information technology in education and science*. https://doi.org/10.28925/9720213284km

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Vadym Abramov
Candidate of technical sciences, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-8026-1475
v.abramov@kubg.edu.ua

Oksana Hlushak
Phd, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-9849-1140
o.hlushak@kubg.edu.ua

Anhelina Plokha
Student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0003-5327-999X
ayplokha.fitu21@kubg.edu.ua

Dovzhenko Timur
Phd, Associate Professor,Associate Professorof the Departmentof Software Engineering
State Universityof Informationand Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0006-9930-5091
timurdov@ukr.net

DESIGNING NETWORK INFRASTRUCTURE WITH CYBERSECURITY REQUIREMENTS IN MIND: APPROACHES AND IMPLEMENTATION BASED ON CISCO

Abstract. The article presents a comprehensive study of modern approaches to designing network infrastructure with regard to cybersecurity requirements, with a focus on practical implementation using Cisco technologies. In the context of growing digital threats and the complexity of information systems, the integration of protection mechanisms at the early stages of design is of particular importance. The concepts of Security-by-Design, Zero Trust architecture, micro-segmentation, and the use of digital twins for simulation testing are considered. It is shown that the implementation of the principle ‘never trust, always verify’ allows localising security incidents, reducing the risks of horizontal spread of attacks, and ensuring constant access control. Considerable attention is paid to building a multi-level network architecture using VLANs, ACLs, WPA3, Port Security, and local authentication. In the Cisco Packet Tracer environment, a star-shaped network with nine logical segments serving up to 300 users with high requirements for bandwidth, connection stability, and data protection is modelled. Scenarios for filtering incoming traffic, protecting wireless access points, and organising backups with the protection of transmitted data via FTP with authentication are proposed. The results confirm the feasibility of applying an integrated approach that ensures compliance with current information security standards. Prospects for further research are related to the adaptation of the described methods for industries with increased cybersecurity requirements.

Keywords: network infrastructure; cybersecurity; network design; Cisco; information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Cisco. (2025, June). *Cisco unveils secure network architecture to accelerate workplace AI transformation*. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m06/cisco-unveils-secure-network-architecture-to-accelerate
2. Syrovatchenko, M. (2024). Legal aspects of cybersecurity in ukraine: current challenges and the role of national legislation. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 1*(41), 314–320. https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/sirovatchenko41.pdf
3. Smith, B. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Security. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war

4. Microsoft. (2022). *The hybrid war in Ukraine*. Microsoft . https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
5. Bellamkonda, S. (2023). Cybersecurity and network engineering: Bridging the gap for optimal protection. *International Journal of Innovative Research in Science, Engineering and Technology*. https://doi.org/10.15680/ijirset.2023.1204007
6. Granata, D., & Rak, M. (2023). Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. *Software Quality Journal, 32*, 125–161. https://doi.org/10.1007/s11219-023-09634-4
7. Diamantopoulou, V., & Mouratidis, H. (2018). A security analysis method for industrial internet of things. *IEEE Transactions on Industrial Informatics, 14*, 4093–4100. https://doi.org/10.1109/TII.2018.2832853
8. Colajanni, M., Zanasi, C., & Russo, S. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks, 156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414
9. Gehrmann, C., & Gunnarsson, M. (2020). A digital twin based industrial automation and control system security architecture. *IEEE Transactions on Industrial Informatics, 16*, 669–680. https://doi.org/10.1109/TII.2019.2938885
10. Masi, M., Aranha, H., Sellitto, G., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling, 22*, 689–707. https://doi.org/10.1007/s10270-022-01075-0
11. Li, L., Gao, S., Zhang, W., Wu, J., Liu, Y., Xia, Y., & Zhang, H. (2024). Toward autonomous trusted networks – From digital twin perspective. *IEEE Network, 38*, 84–91. https://doi.org/10.1109/MNET.2024.3353180
12. Bravo-Haro, M., Broo, D., & Schooling, J. (2022). Design and implementation of a smart infrastructure digital twin. *Automation in Construction*. https://doi.org/10.1016/j.autcon.2022.104171
13. Chen, L., Ni, Y., Huang, D., He, Y., & X., Y. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2022/6476274
14. Liu, J., Liu, G., Meng, L., Wang, Q., & Kang, H. (2023). Theory and application of zero trust security: A brief survey. *Entropy, 25*. https://doi.org/10.3390/e25121595
15. Sarkar, S., Choudhary, G., Hussain, A., Kim, H., & Shandilya, S. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability, 14*(18), 11213. https://doi.org/10.3390/su141811213
16. Syed, N., Anwar, A., Shah, S., Doss, R., Shaghaghi, A., & Baig, Z. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679
17. Hewage, C., Rawindaran, N., Prakash, E., & Jayal, A. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet, 13*, 186. https://doi.org/10.3390/fi13080186
18. Feng, D. (2024). The basics of creating secure data architectures for financial organizations. *The American Journal of Engineering and Technology*. https://doi.org/10.37547/tajet/volume06issue12-13
19. Aladwan, M., Alawadi, S., Awaysheh, F., Cabaleiro, J., Alazab, M., & Pena, T. (2021). Security by design for big data frameworks over cloud computing. *IEEE Transactions on Engineering Management, PP*, 1–18. https://doi.org/10.1109/TEM.2020.3045661
20. Cisco. (n.d.). *What is network segmentation?* https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html
21. National Institute of Standards and Technology. (n.d.). *Defense in depth*. https://csrc.nist.gov/glossary/term/defense_in_depth
22. Verkhovna Rada of Ukraine. (2010). Zakon Ukrainy "Pro zakhyst personal′nykh danykh" № 2297-VI vid 01.06.2010 [Law of Ukraine "On personal data protection" No. 2297-VI dated 01.06.2010]. https://zakon.rada.gov.ua/laws/show/2297-17#Text
23. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
24. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
25. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
26. Abamov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., ... Yaskevych, V. (2021). *Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km*