КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1030
УДК 004.056

**Гарасимчук Олег Ігорович**
к.т.н.,доцент кафедри захисту інформації
Національний Університет "Львівська політехніка", Львів, Україна
ORCID: 0000-0002-8742-8872
*oleh.i.harasymchuk@lpnu.ua*

**Касаткін Юрій Миколайович**
Студент кафедри захисту інформації
Національний Університет "Львівська політехніка", Львів, Україна
*yurii.kasatkin.mkbur.2025@lpnu.ua*

# РОЗМЕЖУВАННЯ ЕЛЕКТРОННОЇ КОМУНІКАЦІЙНОЇ СИСТЕМИ МЕРЕЖІ ТА ЕЛЕКТРОННОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ В УМОВАХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЙ

**Анотація.** У сучасних умовах цифрової трансформації організацій зростає складність та взаємозалежність між електронними комунікаційними мережами (ЕКМ) і електронними інформаційними системами (ЕІС), що підвищує ризики кібератак та порушення конфіденційності, цілісності й доступності даних. Недостатнє розмежування між цими двома рівнями IT-інфраструктури створює умови для розповсюдження загроз у межах єдиного інформаційного простору, зокрема під час атак типу lateral movement або privilege escalation. У статті запропоновано методологію багаторівневого розмежування ЕКМ та ЕІС як ключового напряму підвищення кіберстійкості організацій. Модель базується на принципах мережевої сегментації, ізоляції інформаційних доменів, контролю доступу на основі ролей RBAC та концепції нульової довіри - Zero Trust Architecture. Проведено аналітичне моделювання впливу сегментації на показники безпеки, ймовірність компрометації критичних вузлів, середній час до інциденту та площу атаки. Результати симуляції показали, що впровадження моделі розмежування дозволяє зменшити кількість скомпрометованих вузлів на 25-30%, знизити ймовірність компрометації критичних зон на понад 20% та збільшити середній час до компрометації майже на 50%. Розроблена методика може бути використана як основа для формування політик інформаційної безпеки в державних і корпоративних структурах, а також для побудови інтегрованих систем захисту на основі принципів гнучкої сегментації та управління довірою.

**Ключові слова:** кібербезпека, електронна комунікаційна мережа, електронна інформаційна система, сегментація мережі, Zero Trust, ізоляція сервісів, управління доступом.

## ВСТУП

У сучасному цифровому середовищі організації все більше залежать від високого рівня зв'язності між електронною комунікаційною мережею ЕКМ та електронною інформаційною системою ЕС, що створює значні виклики для забезпечення їхньої кібербезпеки. Надмірна інтеграція мережевих і прикладних компонентів призводить до розширення площі атаки: компрометація одного елемента може слугувати “вхідними дверима” для проникнення в інші підсистеми [1]. Тому питания сегрегації мережі, ізоляції сервісів та чіткого розмежування між мережею і системою набуває ключового значення в сучасному кіберзахисті.

Дослідження свідчать, що підходи типу мережевої сегментації та мікросегментацій значно знижують можливість lateral movement (переміщення зловмисника в межах мережі) і підвищують швидкість виявлення інцидентів [2]. Крім того, архітектура "нульової довіри" - Zero Trust, базується на принципі "ніколи не довіряй, завжди перевіряй" та передбачає постійну верифікацію кожного з'єднання чи запиту, незалежно від того, чи походить він з середини мережі чи ззовні [3]. Водночас багато організацій не реалізують чіткого розмежування між ЕКМ та ЕІС, що створює умови для посилення ризиків, особливо в мультихмарних середовищах, серед середніх та малих підприємств [4].

***Метою даної роботи*** є розроблення методики та моделі розмежування ЕКМ й ЕІС в ІТ-інфраструктурі організацій як складової стратегій підвищення їхньої кіберстійкості. Для досягнення мети необхідно вирішитин наступні завдання: проаналізувати існуючі підходи до архітектурної сегментації мереж і розмежування інформаційних систем, визначити технічні та організаційні критерії, проведення розмежування, сформувати моделі зон довіри та канали взаємодії між сегментами, провести аналітичну оцінку впливу розмежування на ключові показники безпеки, наприклад, площу атаки, ймовірність компрометації, середній час виявлення інциденту, а також надати практичні рекомендації для впровадження моделі в організаціях різного типу.

Запропонований підхід повинен мати як теоретичне значення для систематизації підходів до розмежування мережі та інформаційної системи, так і практичну цінність, щоб можна було оцінити ефективність ізоляції мережевих і інформаційних компонентів у контексті кібербезпеки.

## ПОСТАНОВКА ЗАВДАННЯ

Розвиток електронних комунікаційних мереж і електронних інформаційних систем створює нові виклики у сфері кібербезпеки, зокрема щодо їх взаємодії, управління доступом та контролю інформаційних потоків. Незважаючи на різну функціональну природу цих компонентів - мережа відповідає за транспортування даних, а інформаційна система за їх обробку та зберігання у більшості організацій вони залишаються слабо розмежованими. Це призводить до зростання ризиків уразливості, особливо під час атак із горизонтальним переміщенням зловмисника – lateral movement ra експлуатації внутрішніх ресурсів [5],[6].

Міжнародні дослідження вказують, що в якості основного джерела понад 60% кіберінцидентів у корпоративному секторі є відсутність чіткої мережевої сегментації та ізоляції критичних сервісів [7]. Водночас рекомендації, викладені в NIST SP 800-207 (Zero Trust Architecture), прямо підкреслюють необхідність незалежного контролю доступу між комунікаційною мережею та інформаційними доменами [8]. Тобто сучасна концепція кіберзахисту переходить від реактивного до превентивного підходу, в основі якого лежить принцип функціонального розмежування компонентів.

Для формування дієвої архітектури кіберзахисту організацій постає завдання визначення чіткої межі між ЕКМ і ЕІС, розроблення моделі взаємодії між ними та розроблення системи контролю потоків даних і доступу. Такий підхід дозволяє мінімізувати ймовірність ескалації привілеїв, знизити площу атаки та підвищити загальний рівень кіберстійкості організації.

Процес виконання кожного поставленого завдання для досягнення мети дослідження повинен закінчуватися певним результатом як це відображено на *Рис. 1*:

| | |
|---|---|
| **Аналіз** | • Провести аналіз сучасних підходів до сегментації, ізоляції та Zero Trust-архітектур у контексті кібербезпеки організацій. |
| **Критерії** | • Визначити технічні, логічні та організаційні критерії проведення розмежування між ЕКМ та ЕІС. |
| **Концептуальна модель** | • Визначити технічні, логічні та організаційні критерії проведення розмежування між ЕКМ та ЕІС. |
| **Аналітична модель** | • Запропонувати аналітичну модель оцінювання ефективності розмежування через показники безпеки імовірність компрометації, середній час виявлення інциденту (MTTD) та площу атаки. |
| **Аналітичне моделювання** | • Провести порівняльний аналіз сценаріїв із розмежуванням та без нього, оцінюючи вплив запропонованої моделі на рівень захищеності ІТ-інфраструктури. |
| **Рекомендації** | • Надати рекомендації щодо впровадження моделі в корпоративних і державних інформаційних системах з урахуванням їх масштабності, регуляторних вимог та ресурсних обмежень. |

*Рис. 1. Поставлені завдання та основні результати*

Розв'язання цих завдань забезпечить практичну основу для побудови стійкої системи кіберзахисту, у якій електронна комунікаційна мережа та електронна інформаційна система функціонуватимуть у межах чітко визначених зон безпеки. Це дозволить реалізувати принцип мінімізації довіри, зменшити вплив людського фактора та запобігти каскадному поширенню атак у середині інфраструктури.

**Теоретичні основи розмежування ЕКМ та ЕІС**

В основі сучасної концепції кібербезпеки лежить принцип поділу IT-інфраструктури на ізольовані компоненти, кожен з яких виконує чітко визначену функцію. Такий підхід дає змогу мінімізувати ризики компрометації системи загалом, навіть якщо один елемент зазнав зламу. Ефективне розмежування електронної комунікаційної мережі та електронної інформаційної системи е одним із базових елементів цієї архітектури [9].

Електронна комунікаційна мережа – це сукупність апаратних та програмних засобів, що забезпечують передавання, маршрутизацію та обмін електронними даними між користувачами, сервісами й системами. Її функціональність охоплює транспортний рівень взаємодії, керування трафіком, шифрування каналів, моніторинг мережевих подій та підтримку протоколів безпечного зв'язку [10].

Електронна інформаційна система, у свою чергу, функціонує на прикладному рівні та включає сервіси з обробки, зберігання та управління інформаційними ресурсами бази даних, аналітичні системи, веб-портали, системи управління документами [11].

Попри очевидні відмінності, у більшості сучасних організацій ці дві складові, як правило, тісно інтегровані, що ускладнює ефективне управління ризиками. Відсутність межі між транспортним та прикладним рівнями часто створює умови для згаданого вище lateral movement – тобто горизонтального переміщення атакуючого після первинного проникнення в мережу [12]. У таких умовах ізоляція критичних сегментів і впровадження міжрівневої перевірки запитів стає ключовим завданням кіберзахисту.

**Підходи до розмежування та сегментації**

Серед основних концепцій, які визначають логіку поділу IT-інфраструктури, виділяють мережеву сегментацію, мікросегментацію та архітектуру нульової довіри Zero Trust.

Мережева сегментація – це логічний або фізичний поділ інфраструктури на підмережі з обмеженими каналами взаємодії, які контролюються міжмережевими екранами або маршрутизаторами з політиками доступу. Такий підхід дозволяє обмежити обсяг ресурсів, доступних потенційному зловмиснику [13].

Мікросегментація, на відміну від традиційної, реалізує більш гнучке, програмно-визначене керування потоками даних – Software-Defined Networking або SDN, це коли кожен вузол або додаток може бути розміщений у власній ізольованій зоні з окремими правилами безпеки (14).

Архітектура Zero Trust, описана у NIST SP 800-207, виходить із припущення, що жоден користувач або пристрій не може бути апріорі довіреним навіть якщо він перебуває всередині корпоративної мережі. Доступ надається лише після автентифікації, авторизації та оцінки контексту, наприклад, геолокації, типу пристрою, рівня ризику [15]. Цей підхід фактично нівелює межу між внутрішнім та зовнішнім середовищем, замінюючи її динамічним контролем довіри на всіх рівнях.

**Розмежування ЕКМ та ЕІС як елемент моделі "Defense in Depth"**

Модель Defense in Depth передбачає багаторівневий підхід до захисту, де кожен рівень: мережевий, транспортний, прикладний та інформаційний має власні механізми безпеки. Розмежування ЕКМ і ЕІС фактично реалізує цей принцип: мережеві засоби, фаєрволи, шлюзи, IDS/IPS – забезпечують контроль трафіку, а інформаційна система – політики автентифікації, криптографічного захисту й моніторингу подій [16].

Синергія цих рівнів дозволяє створити архітектуру, в якій навіть при компрометації одного сегмента решта систем залишаються функціонально незалежними. Крім того, ізоляція забезпечує кращу відповідність нормативним вимогам – ISO/IEC 27033-1:2015

наголошує, що логічне розмежування мережевих та прикладних сервісів є обов'язковою складовою комплексної інформаційної безпеки [17].

**Проблеми та виклики впровадження**

Попри очевидні переваги, практична реалізація розмежування має низку труднощів основними з яких є:

–складність інтеграції з уже наявними інфраструктурами, побудованими за монолітною моделлю;

–висока вартість впровадження мікросегментації у великих середовищах;

–відсутність кваліфікованих фахівців для адміністрування Zero Trust: політик;

–конфлікти між вимогами безпеки та зручністю користувачів [18].

Тому сучасні дослідження спрямовані на розроблення динамічних моделей сегментації, що адаптуються до контексту користувача, навантаження мережі та рівня ризику. Такі моделі поступово впроваджуються в державному секторі, промислових системах ICS/SCADA та хмарних середовищах [19-20]. Додатково зростає інтерес до автоматизованих механізмів, які зменшують складність управління сегментацією.

Отже, розмежування ЕКМ та ЕІС є ключовою складовою формування кіберстійких архітектур, що поєднують принципи багаторівневого захисту, мінімальної довіри та адаптивного управління доступом.

## Методика розмежування електронної комунікаційної мережі та електронної інформаційної системи

**Основні етапи проведення розмежування**

Ефективне розмежування електронної комунікаційної мережі та електронної інформаційної системи передбачає комплексний підхід, який схоплює технічні, організаційні та аналітичні аспекти управління ІТ-інфраструктурою. Методика, запропонована в межах цього дослідження, базується на принципах Zero Trust Architecture, Defense in Depth і рекомендаціях NIST SP 800-207 та ISO/IEC 27033-1:2015 [21-22].

*Крок 1. Інвентаризація активів і потоків даних*

Першим етапом є створення детального реєстру активів і карти потоків даних. Згідно з рекомендаціями NIST SP. 800-137 Information Security Continuous Monitoring, саме повна інвентаризація є передумовою для визначення меж безпеки [23].

На цьому етапі необхідно:

–ідентифікувати всі вузли ЕКМ: маршрутизатори, комутатори, шлюзи, сервери зв'язку;

–класифікувати компоненти ЕІС: бази даних, інформаційні сервіси, аналітичні модулі, CRM/ERP системи;

–визначити критичні канали обміну: внутрішні API, зовнішні з'єднання, служби синхронізації;

–побудувати топологічну карту потоків даних між ЕКМ та ЕІС

Результатом етапу є інвентаризаційна модель ІТ-інфраструктури, що дає змогу виявити потенційні точки перетину мережевих і прикладних шарів, очкільки саме вони є осередками можливих уразливостей [24].

*Крок 2.Моделювання зон довіри*

Після ідентифікації активів здійснюється побудова моделі зон довіри, що визначає рівень доступу та безпеки для кожного сегмента системи.

Найпоширенішою структурою є чотирьохрівнева модель:

–Зовнішнє середовище: інтернет, партнери, віддалені користувачі;

–Буферна зона для розміщення публічних сервісів: веб-портали, поштові шлюзи, API-вузли;

–Внутрішня корпоративна мережа;

–Сегмент критичних інформаційних систем і баз даних.

Кожна зона ізолюється від іншої через міжмережеві екрани, IDS/IPS-системи та шлюзи рівня додатків. Такий підхід відповідає принципам Network Segmentation Framework (Cisco Systems, 2022) [25].

*Крок 3. Виділення функціональних доменів*

На цьому етапі проводиться логічний поділ ресурсів за функціональним призначенням. Виділяють такі домени:

–User Domain – робочі станції користувачів, термінальні клієнти, мобільні пристрої;

–Service Domain – сервери додатків, файлові сховища, аналітичні служби;

–Management Domain системи централізованого керування, моніторингу, резервного копіювання;

–Information System Domain – ядро прикладних систем, бази даних, внутрішні API.

Такий поділ дозволяє застосовувати політики доступу на основі ролей RBAC або атрибутів ABAC відповідно до вимог ISO/IEC 27001:2022 [26].

*Крок 4. Розмежування каналів обміну*

Ключовим елементом методики є визначення та обмеження каналів обміну між EKM та EIC. Для цього застосовуються:

–проксі-сервери для фільтрації та кешування HTTP/HTTPS-трафіку;

–фаєрволи для обмеження портів, протоколів і напрямків зв'язку;

–API Gateway для контролю викликів між сервісами, авторизації та шифрування запитів;

–шлюзи безпеки електронної пошти SEG – перевірка вкладень і посилань на шкідливі ресурси.

Розмежування каналів має базуватись на принципі least privilege – кожен компонент отримує мінімально необхідний набір зв'язків для виконання своєї функції [27].

*Крок 5. Контроль доступу та автентифікації*

Система управління доступом реалізується на рівнях мережі, сервісів і прикладних додатків. Використовуються:

–Role-Based Access Control (RBAC) – призначення прав доступу за ролями;

–Attribute-Based Access Control (ABAC) – контекстуальне визначення прав

–Multi-Factor Authentication (MFA) – багатофакторна автентифікація;

–Network Access Control (NAC) – перевірка стану пристрою перед підключенням.

Такі механізми відповідають рекомендаціям NIST SP 800-162 (Guide to Attribute-Based Access Control) [28] та ENISA (Access Control in Digital Environments, 2023) [29].

*Крок 6. Моніторинг та журналювання*

Останній етап - впровадження централізованих систем моніторингу та реагування на інциденти: Security Information and Event Management (SIEM) і Security Operations Center (SOC). Вони здійснюють збір, кореляцію та аналіз подій з різних сегментів EKM та EIC.

Моніторинг повинен охоплювати:

–аномалії у мережевих з'єднаннях;

–несанкціоновані спроби доступу до сервісів EIC;

–події автентифікації та авторизації;

–зміну конфігурацій або політик безпеки.

Відповідно до ENISA Threat Landscape Report 2023, саме централізоване журналювання дозволяє скоротити середній час виявлення інцидентів MTTD до 35%, порівняно з розподіленими рішеннями [30].

**Візуалізація моделі розмежування та опис моделі ризиків**

**Схема моделі**

Візуальна модель розмежування ЕКМ та ЕІС згідно із описаною вище методикою, представлена на Рис. 2.

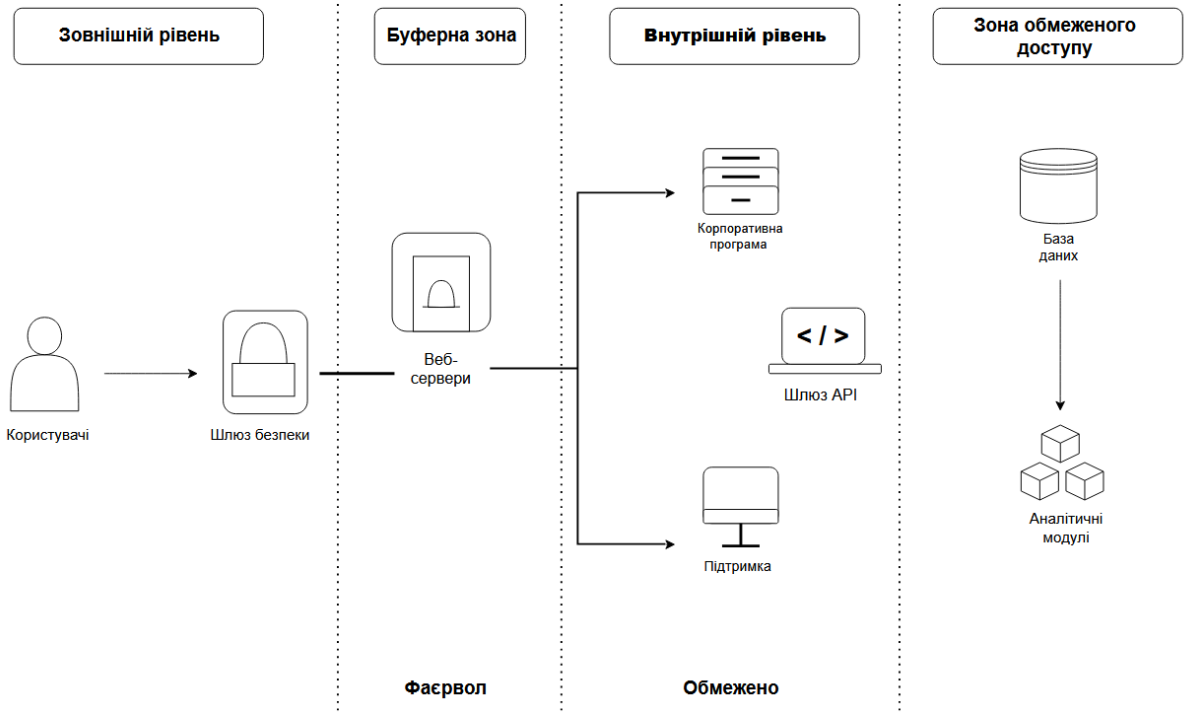


*Рис. 2. Схема моделі*

Дана модель побудована за принципом багаторівневої ізоляції з чітким визначенням меж між зонами довіри, каналами обміну та системами контролю доступу.

Модель включає чотири основні рівні безпеки, що відповідають архітектурі "External - DMZ - Internal -Restricted":

1. Зовнішній рівень (External Zone) – це рівень користувачів, які підключаються через інтернет. Взаємодія відбувається через захищений шлюз доступу (Secure Gateway), який реалізує TLS-шифрування, перевірку сертифікатів та попередню автентифікацію,
2. Буферна зона (DMZ) використовується для розміщення публічних сервісів: веб-портали, API-вузли. DMZ ізольована від внутрішньої мережі за допомогою двох фаєрволів різного класу (Dual-Firewall Model), що унеможливлює пряме перенесення трафіку ззовні до внутрішніх систем [31].
3. Внутрішній рівень (Internal Zone) забезпечує взаємодію служб підтримки, користувачів та корпоративних додатків. Тут впроваджено Network Access Control (NAC), а також політики RBAC/ABAC для диференційованого доступу до сервісів і даних [32].
4. Зона обмеженого доступу (Restricted Zone) містить ядро ІС: бази даних, аналітичні модулі – критичні ресурси. Доступ до цієї зони можливий лише

через API Gateway або захищений тунель після багатофакторної автентифікації (MFA).

Усі транзакції контролюються SIEM-системою, а журнали подій надходять до SOC-центру для аналізу аномалій [33].

Між зонами діють односторонні шлюзи (unidirectional gateways) для передавання даних лише в безпечному напрямку, наприклад, від EIC до моніторингових систем, але не навпаки, що відповідає принципу unidirectional data diode [34].

**Опис моделі ризиків**

У межах цієї моделі доцільно виділити кілька критичних напрямів впливу сегментації на загальний рівень безпеки, зокрема зменшення lateral movement та обмеження privilege escalation.

*Зниження ймовірності lateral movement*

У традиційних архітектурах мережеві сегменти часто мають спільні облікові записи або сервіси, через що зловмисник після первинного проникнення може вільно переміщуватися між системами.

У розмежованій архітектурі lateral movement мінімізується завдяки:

– мікросегментації трафіку між зонами SDN-контроль доступу;
– ізоляції доменів автентифікації, окремі служби LDAP/Kerberos для внутрішніх і зовнішніх зон;
– політикам just-in-time access, тимчасові сесії замість постійних привілеїв;
– системам поведінкового моніторингу (UEBA), які фіксують нетипову активність користувачів [35].

За результатами дослідження IBM Cost of a Data Breach 2023, компанії, що впровадили сегментацію на рівні Zero Trust, зменшили середню площу атаки на 43% [36].

*Обмеження privilege escalation*

Ескалація привілеїв уразлива тоді, коли різні рівні системи мають спільну базу облікових записів або привілеї адміністратора.

У розмежованій архітектурі доступ до зон Internal та Restricted регулюється незалежними механізмами авторизації та журналювання.

Для адміністраторів використовується Privileged Access Management (PAM) рішення, які обмежують час дії сеансу, автоматично відкликають права після виконання задачі та зберігають повний відео журнал дій [37].

*Зниження ризику ланцюгових атак*

Ізоляція потоків між зонами не дозволяє зловмиснику використовувати скомпрометовану службу як "міст" до критичних ресурсів.

Використання API Gateway і Reverse Proxy забезпечує додатковий контроль запитів, блокуючи аномальні патерни, що відповідає рекомендаціям OWASP API Security Top-10 (2023) [38].

*Підвищення стійкості до внутрішніх загроз*

Розмежування дозволяє реалізувати принцип segregation of duties – розподіл відповідальності між адміністраторами мережі, додатків та баз даних. Це мінімізує вплив людського фактора і внутрішніх зловживань. ENISA (2023) зазначає, що багаторівневий розподіл привілеїв зменшує ризик інсайдерських інцидентів на 30-40% [39].

Запропонована модель візуально і логічно демонструє, як фізичне та логічне розмежування зон EKM і EIC підвищує загальну кіберстійкість організації.

Її впровадження забезпечує зменшення ймовірності компрометації критичних систем, скорочення часу реагування на інциденти MTTR та покращення відповідності міжнародним стандартам ISO/IEC 27001 і NIST SP 800-207.

**Практичне дослідження та модельна симуляція**

Мета практичного дослідження розглянутої методики полягає в оцінюванні ефективності розмежування ЕКМ та ЕІС у контексті забезпечення кібербезпеки організації. Для цього проведено аналітичну симуляцію, яка моделює динаміку поширення кіберзагроз у двох сценаріях базовому, тобто із низьким рівнем сегментації, та розмежованому із впровадженими зонами довіри, засобами контролю доступу та виявлення інцидентів.

Основним завданням дослідження є кількісна оцінка впливу мережевої сегментації та функціонального поділу ІТ-системи на ключові показники безпеки: ймовірність компрометації критичних зон, середню кількість уражених вузлів та середній час до компрометації критичних елементів.

**Методика проведення симуляції**

Для реалізації модельного дослідження використано підхід стохастичного моделювання процесу розповсюдження компрометації в мережі, реалізований через метод Монте-Карло.

Модель представлено у вигляді орієнтованого графа G(V, E), де вершини V це вузли мережі: сервери, клієнти, шлюзи, бази даних, а ребра E – канали взаємодії або потенційні шляхи поширення атаки. Модель складається з чотирьох зон довіри:

- зовнішня (External) – клієнти, постачальники, віддалені користувачі;
- демілітаризована зона (DMZ) – веб-сервери, API-шлюзи;
- внутрішня (Internal) – корпоративні сервіси, служби управління;
- критична (Restricted) – сховища даних, аналітичні системи, об'єкти з підвищеним рівнем контролю.

Поширення атаки моделювалось як стохастичний процес типу марковського ланцюга, де кожен вузол може перебувати в одному з чотирьох станів: secure (захищений), compromised (скомпрометований), detected (виявлений), remediated (відновлений). Ймовірності переходів між станами визначались через параметри:

- $P_{init}$ – початкова ймовірність проникнення у зовнішню зону;
- $P_{move}$ – імовірність поширення компрометації на сусідній вузол;
- $\lambda_{detect}$ – інтенсивність виявлення: Mean Time To Detec;
- $\mu_{remed}$ – інтенсивність відновлення: Mean Time To Remediate.

Для кожного сценарію проведено 2000 симуляцій, у межах яких відтворювався процес поширення атаки протягом 240 умовних хвилин.

**Початкові параметри та налаштування моделі**

Параметри симуляції наведено у Таблиця 1.

*Таблиця 1.*

***Основні параметри моделі для двох сценаріїв***

| Параметр | Позначення | Базовий сценарій | Розмежований сценарій |
|---|---|---|---|
| Початкова ймовірність проникнення | $P_{init}$ | 0.02 | 0.02 |
| Імовірність поширення між зонами | $P_{move\_inter}$ | 0.6 | 0.12 |
| Імовірність поширення в межах зони | $P_{move\_intra}$ | 0.4 | 0.25 |
| Інтенсивність виявлення (1/MTTD) | $\lambda_{detect}$ | 0.04 | 0.08 |
| Інтенсивність відновлення (1/MTTR) | $\mu_{remed}$ | 0.02 | 0.024 |

Наведені в таблиці параметри використовувалися як вхідні змінні моделі, що визначають поведінку марковського процесу поширення атаки. Значення цих параметрів були встановлені на основі структурних відмінностей між двома архітектурними сценаріями – базовим та розмежованим.

Параметри базового сценарію відображають характерну для традиційної мережі ситуацію, у якій відсутні механізми сегментації, а міжзонна та внутрішньозонна взаємодія залишається відносно вільною. Тому ймовірності поширення між зонами (P_move_inter) та всередині зони (P_move_intra) мають вищі значення, а інтенсивності виявлення (λ_detect) та відновлення (μ_remed) нижчі через слабшу інтеграцію засобів моніторингу та реакції.

Для розмежованого сценарію параметри були скориговані відповідно до ефектів, які згідно з літературою та архітектурними підходами забезпечує мережна сегментація:

– зменшення міжзонного трафіку через мікросегментацію, NAC, API Gateway та міжмережеві екрани;

– прискорення виявлення інцидентів завдяки системам SIEM/SOC;

– покращення процесів відновлення через автоматизацію та контроль привілейованих доступів.

Отже, параметри обох сценаріїв – це вихідні умови моделі та використовуються для подальшого статистичного моделювання. Саме на їх основі у наступних кроках були проведені 2000 симуляцій, результати яких наведені у другій таблиці.

**Результати симуляції**

За результатами 2000 ітерацій моделювання поширення атаки на основі параметрів, визначених для двох архітектурних сценаріїв для кожного сценарію отримано узагальнені статистичні показники (Таблиця 2). Для кожного сценарію було проведено 2000 симуляцій марковського процесу, у межах яких моделювався розвиток інциденту протягом 240 умовних хвилин. Під час кожного прогону система фіксувала кількість скомпрометованих вузлів, час першої компрометації зони Restricted, тривалість інциденту та інші показники, після чого обчислено їх статистично усереднені значення.

*Таблиця 2.*

**Порівняльні результати симуляції**

| Показник | Базовий сценарій | Розмежований сценарій | Зміна, % |
|---|---|---|---|
| Ймовірність компрометації зони Restricted, [$P_{full}$] | 0.869 | 0.688 | -20.8% |
| Середня кількість скомпрометованих вузлів, E[$n_{comp}$] | 75.80 | 54.23 | -28.5% |
| Середній час до першої компрометації, Restricted (хв) | 118.2 | 173.6 | +46.9% |
| Середній час до виявлення інциденту (хв) | 103.5 | 98.0 | -5.3% |

Отримані дані показують, яким чином архітектурні відмінності впливають на стійкість системи до кібератак. Зокрема, розмежований сценарій демонструє зниження середньої кількості скомпрометованих вузлів на 28,5%, що свідчить про ефективність мікросегментації та обмеження міжзонного руху атаки. Водночас спостерігається збільшення середнього часу до першої компрометації зони Restricted на 46,9%, що вказує на покращене стримування та уповільнення розвитку атакуючої активності. Відносно

невелике скорочення часу до завершення інциденту (–5,3%) відображає ефект пришвидшеного виявлення та відновлення у розмежованій архітектурі.

Для покращення сприйняття даних та візуального аналізу нижче наведено стовпчасті діаграми, що графічно ілюструють різницю між показниками базового й розмежованого сценаріїв. Графіки дозволяють швидко оцінити масштаб впливу сегментації та чітко продемонструвати ті тенденції, що в таблиці подані у числовій формі.

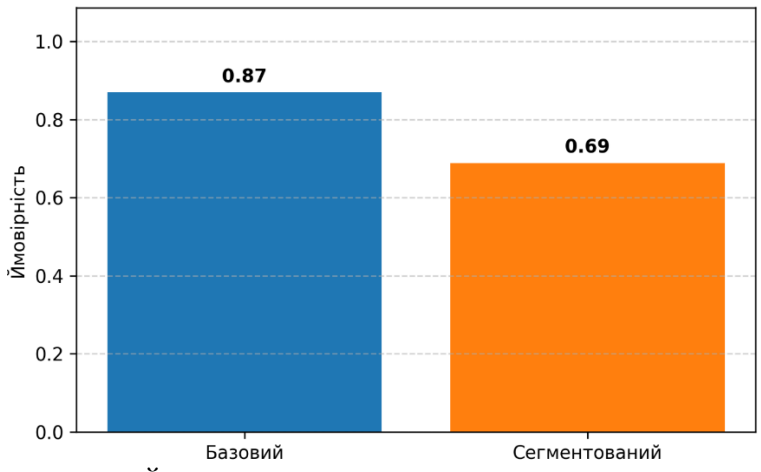


*Рис. 3. Ймовірність компрометації зони Restricted*

Значення на осі ординат подані у частках від 1, тобто 0.87 = 87%, 0.69 = 69%, що узгоджується з форматом вихідних результатів моделі, наведених у попередній таблиці.

Як видно з *Рис. 3*, у сегментованому сценарії ймовірність компрометації критичної зони зменшується з 0.87 до 0.69, тобто на приблизно 20,8%. Це значення отримане шляхом порівняння симульованих результатів, поданих у таблиці “Порівняльні результати симуляції”. Зниження ймовірності свідчить про ефективність додаткової сегментації, яка обмежує горизонтальне поширення загроз завдяки ізоляції зони довіри.

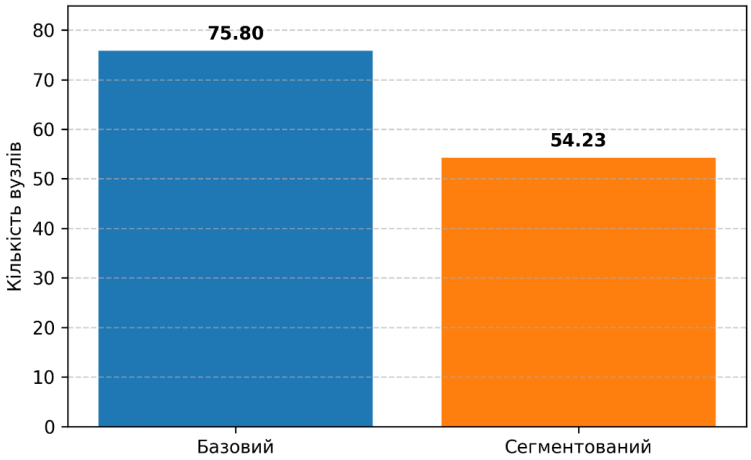


*Рис. 4. Середня кількість скомпрометованих вузлів*

Значення на осі ординат подані як абсолютна кількість вузлів, не у відсотках, що відповідає формату вихідних даних симуляції, наведених у таблиці “Порівняльні результати симуляції”.

Як показано на Рис. 4, середня кількість скомпрометованих вузлів зменшується з 75.80 до 54.23. Це означає скорочення на приблизно 28.5%, що розраховано відповідно до значень у таблиці (75.80−54.23)/75.80 ≈ 0.285. Така різниця підтверджує зменшення загальної площі атаки (*attack surface*) системи: у разі успішної початкової компрометації менша кількість внутрішніх компонентів залучається до подальшого поширення атаки.

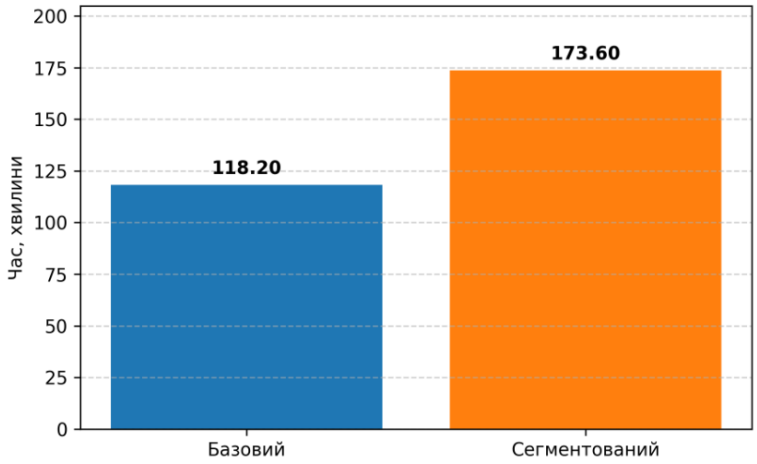


*Рис. 5. Середній час до першої компрометації зони*

Згідно з Рис. 5 середній час до першої компрометації критичної зони зріс з 118,2 до 173,6 хвилин +46,9%. Отже, впровадження сегментації надає додатковий часовий інтервал, який може бути використаний для виявлення інциденту й запобігання його подальшому поширенню.

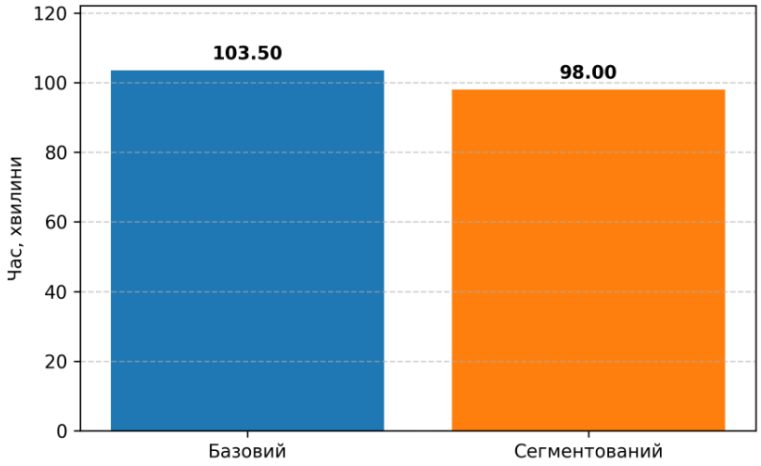


*Рис. 6. Середній час до виявлення інциденту MTTD*

На Рис. 6 наведено середній час до виявлення інциденту MTTD, який у розмежованій архітектурі скоротився несуттєво -5,3%. Це може бути пов'язано з тим, що ефективність моніторингу не залежить лише від структурних характеристик мережі, а також від налаштувань системи журналювання та аналітики подій.

**Інтерпретація результатів і висновки**

Результати модельної симуляції свідчать, що розмежування EKM та EIC має позитивний вплив на стійкість IT-інфраструктури до кібератак. Усі наведені кількісні показники відповідають результатам таблиці “Порівняльні результати симуляції” та

графічним ілюстраціям, що дозволяє однозначно інтерпретувати ефект від впровадження сегментації.

По-перше, ймовірність компрометації критичної зони Restricted знизилась приблизно на 21% (з 0.87 до 0.69). Це підтверджує, що запровадження зон довіри, DMZ, Internal, Restricted, зменшує кількість потенційних маршрутів досягнення критичних активів і обмежує площу атаки.

По-друге, середня кількість уражених вузлів зменшилась на 28.5%, з 75.80 до 54.23. Така динаміка безпосередньо свідчить про зменшення каскадного ефекту зараження: навіть якщо початкове проникнення відбулося, подальше поширення в сегментованому середовищі суттєво обмежується.

По-третє, середній час досягнення критичної зони зріс на 46.9% , з 118.2 до 173.6 хвилин. Це створює додаткове “вікно реагування” для SOC/SIEM-механізмів, збільшуючи ймовірність виявлення та стримування атаки до того, як вона набуде критичного характеру.

Незначне покращення середнього часу виявлення інциденту, а саме зменшення MTTD на 5.3%, пояснюється тим, що в сегментованому середовищі більше ресурсів приділяється моніторингу внутрішніх вузлів, що підвищує точність виявлення, але не завжди суттєво впливає на швидкість.

Узагальнюючи наведені вище результати модулювання, можна зробити висновок, що розмежування ЕКМ та ЕІС є ефективним засобом зниження ризиків кіберкомпрометацій, який забезпечує: обмеження горизонтального руху атакувальників lateral movement, скорочення площі атаки та кількості уражених компонентів, збільшення часу для реагування на інциденти та підвищення загального рівня кіберстійкості організації.

**Обговорення результатів**

Отримані результати моделювання демонструють суттєвий вплив сегментаці мережевої інфраструктури та ЕКМ і ЕІС на стійкість організації до кіберзагроз. Застосована стохастична модель поширення компрометації у вигляді марковського процесу, яка дозволила кількісно оцінити динаміку атаки та визначити ключові показники ефективності обраних архітектурних підходів.

Порівняння базового та сегментованого сценаріїв засвідчило, що запровадження зон довіри, скорочення міжзонних каналів взаємодії та підсилення механізмів виявлення інцидентів призводить до зменшення площі атаки та підвищення складності вертикального прориву до критичних ресурсів. Зокрема, у сегментованому сценарії спостерігається скорочення середньої кількості скомпрометованих вузлів приблизно на 28,5%, що свідчить про обмеження горизонтального латерального розповсюдження загрози. Водночас ймовірність досягнення зони Restricted знижується приблизно на 21%, що підтверджує ефективність бар'єрного контролю доступу та ізоляції критичних компонентів.

Одним із ключових аспектів є збільшення середнього часу до першої компрометації критичної зони з 118,2 до 173,6 хвилин. Це формує додаткове “часове вікно реагування”, у межах якого засоби моніторингу та реагування SOC, SIEM, IDS/IPS, які можуть ініціювати процедури стримування інциденту. Таким чином, сегментація не тільки зменшує інтенсивність поширення атаки, а й підвищує ймовірність вчасного виявлення. Водночас зменшення середнього часу до виявлення MTTD є менш вираженим, що може вказувати на залежність цього показника більше від організаційних процесів реагування, ніж від мережевої архітектури.

Разом із тим результати виявляють і обмеження досліджуваного підходу. Сегментація неминуче підвищує архітектурну складність та вартість обслуговування інфраструктури. Для великих організацій впровадження політик контрольованого доступу, міжмережевих фільтрів, мікросегментації та моніторингу подій потребуватиме додаткових ресурсів SOC та постійної аудиторії мережевих конфігурацій. Водночас у малих середніх організаціях надмірно деталізована сегментація може виявитися невиправданою з погляду співвідношення "вартість/ефективність"

З огляду на це, рекомендовано диференційований підхід до впровадження сегментацій:

*Таблиця 3.*

**Рекомендації**

| Тип організації | Рекомендована стратегія сегментацій |
|---|---|
| Малі та середні підприємства | Віртуальна сегментація VLAN з ACL/Firewall для міжмережевого контролю |
| Великі корпоративні мережі | Мікросегментація на основі SDN/NSX/Zero Trust Network Access |
| Критична інфраструктура та держсектор | Нормативно регульоване фізичне розмежування + SIEM + NAC + PAM |

Таким чином, результати моделювання підтверджують доцільність впровадження структурованої сегментації мережі та розмежування ЕКМ і ЕІС як одного з базових механізмів підвищення кіберстійкості. Модель демонструє не лише зменшення імовірності компрометації критичних ресурсів, але й збільшення можливостей для своєчасного реагування на інциденти, що узгоджується з концепціями Zero Trust та Active Defense.

Отримані результати можуть бути використані для обґрунтування впровадження архітектурних рішень типу Zero Trust Network або мікросегментації корпоративних мереж, що є сучасним трендом у забезпеченні інформаційної безпеки критичних систем.

## ВИСНОВКИ

У роботі проведено дослідження впливу розмежування електронної комунікаційної мережі та електронної інформаційної системи на рівень кіберстійкості організаційної інфраструктури. На основі побудованої стохастичної моделі поширення компрометації було реалізовано симуляцію за методом Монте-Карло, що дозволило кількісно оцінити динаміку кіберінциденту у двох архітектурних сценаріях: базовому та сегментованому.

Результати моделювання засвідчили, що впровадження зон довіри, обмеження міжзонних каналів взаємодії та підсилення засобів контролю доступу дозволяють істотно зменшити ризики масштабної компрометації. У порівнянні з базовою архітектурою сегментований сценарій забезпечує:

- зниження ймовірності компрометації критичної зони приблизно на 21%;
- скорочення середньої кількості скомпрометованих вузлів майже на 28,5%;
- збільшення середнього часу досягнення зони Restricted на понад 47%, що створює додаткове "вікно реагування" для команд моніторингу та реагування на інциденти.

Таким чином, розмежування ЕКМ та ЕІС не лише зменшує площу атаки й ускладнює латеральне проникнення, але й підвищує ефективність виявлення та реагування, узгоджуючись із принципами Zero Trust та сучасними підходами до управління кіберризиками.

Разом із тим упровадження сегментації потребує врахування технічних та організаційних обмежень: додаткових витрат на підтримку інфраструктури, розроблення політик доступу та забезпечення безперервного моніторингу. Ефективність підходу значною мірою визначається рівнем зрілості процесів інформаційної безпеки в організації.

Подальші дослідження доцільно спрямувати на:

– розроблення автоматизованих механізмів перевірки коректності сегментації;
– застосування адаптивного контролю доступу на основі поведінкової аналітики;
– інтеграцію інтелектуальних систем кореляції подій та ризик-орієнтованого моніторингу.

Загалом проведене дослідження підтверджує, що сегментація мережі та функціональне розмежування підсистем є ключовим елементом формування кіберстійкої архітектури і повинні розглядатися як обов'язкова складова політики інформаційної безпеки сучасної організації.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kotha, N. R. (2020). Network segmentation as a defense mechanism for securing enterprise networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 11*(3), 3023–3030. https://doi.org/10.61841/turcomat.v11i3.14942
2. Bondhala, S. (2025). Modern defense paradigms: Zero Trust architecture, network segmentation, and micro-segmentation. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/CSEIT25112714
3. Shastri, M. (2025). Understanding Zero-Trust architecture for developing comprehensive cybersecurity protocols. *International Journal of Advanced Research in Cyber Security, 3*(1), 1–4.
4. Santoso, E. (2022). Comparative analysis of network segmentation strategies to counter targeted attacks in global e-commerce cloud infrastructures. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 6*(12), 1–6.
5. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security, 2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1
6. Kaur, P., & Singh, M. (2022). Network segmentation and micro-segmentation in enterprise security architecture. *International Journal of Computer Applications, 183*(47), 22–28. https://doi.org/10.5120/ijca2022922120
7. IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach
8. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
9. Bishop, M. (2018). *Introduction to computer security.* Addison-Wesley. ISBN 978-0-321-24744-2
10. Kurose, J., & Ross, K. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
11. International Organization for Standardization. (2018). *ISO/IEC 27000:2018 — Information security management systems — Overview and vocabulary.* Geneva.
12. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security, 2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1
13. Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *VDE Kongress.* Berlin.
14. Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS)* (pp. 1–7). https://doi.org/10.1109/SDN4FNS.2013.6702553
15. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
16. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST SP 800-145). https://doi.org/10.6028/NIST.SP.800-145
17. International Organization for Standardization. (2015). *ISO/IEC 27033-1:2015 — Network security — Part 1: Overview and concepts.* Geneva.

18. Sedgewick, M. (2021). Challenges in implementing Zero Trust networks. *IEEE Security & Privacy, 19*(3), 72–79. https://doi.org/10.1109/MSEC.2021.3062045
19. Hu, J., & Liu, H. (2022). Dynamic network segmentation for adaptive cyber defense. *Computers & Security, 116*, 102677. https://doi.org/10.1016/j.cose.2022.102677
20. Chandia, R., et al. (2009). Security strategies for SCADA networks. *International Journal of Critical Infrastructure Protection, 2*(1–2), 28–37. https://doi.org/10.1016/j.ijcip.2009.01.002
21. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
22. International Organization for Standardization. (2015). *ISO/IEC 27033-1:2015 — Network security — Part 1: Overview and concepts.* Geneva.
23. National Institute of Standards and Technology. (2011). *NIST SP 800-137: Information security continuous monitoring (ISCM) for federal information systems and organizations.* https://doi.org/10.6028/NIST.SP.800-137
24. Kreibich, T., & Crowcroft, J. (2023). Network topology and data flow mapping for cybersecurity. *Computers & Security, 117*, 102747. https://doi.org/10.1016/j.cose.2023.102747
25. Cisco Systems. (2022). *Network segmentation design guide* (White Paper). https://bookstation.org/book/cisco-ise-design-guide-4987197
26. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva.
27. Kindervag, J. (2010). *Building a Zero Trust network.* Forrester Research.
28. National Institute of Standards and Technology. (2014). *NIST SP 800-162: Guide to attribute-based access control (ABAC) definition and considerations.* https://doi.org/10.6028/NIST.SP.800-162
29. European Union Agency for Cybersecurity. (2023). *Access control in digital environments: Principles and best practices.*
30. European Union Agency for Cybersecurity. (2023). *Threat landscape 2023 — Main trends and emerging threats.*
31. Microsoft Security Architecture Center. (2023). *Zero Trust implementation guidance.* https://learn.microsoft.com/security/zero-trust
32. National Institute of Standards and Technology. (2014). *NIST SP 800-162: Guide to attribute-based access control (ABAC).* https://doi.org/10.6028/NIST.SP.800-162
33. Splunk Inc. (2023). *Security information and event management best practices.* https://www.splunk.com
34. Peterson, R. S. (2019). Unidirectional gateway security models. *IEEE Security & Privacy, 17*(4), 73–80. https://doi.org/10.1109/MSEC.2019.2914368
35. Noor, M., & Hassan, A. (2022). A survey on detection and prevention techniques for lateral movement in enterprise networks. *Computers & Security, 121*, 102859. https://doi.org/10.1016/j.cose.2022.102859
36. IBM Security. (2023). *Cost of a data breach report 2023.* https://www.ibm.com/reports/data-breach
37. CyberArk. (2023). *Privileged access management explained* (White Paper). https://www.cyberark.com/resources
38. OWASP Foundation. (2023). *API Security Top-10 2023.* https://owasp.org/API-Security
39. European Union Agency for Cybersecurity. (2023). *Threat landscape 2023 — Main trends and emerging threats.*

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

**Harasymchuk Oleh Ihorovych**
PhD, Associate Professor, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8742-8872
*oleh.i.harasymchuk@lpnu.ua*

**Kasatkin Yurii Mikolayovich**
Student, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
*yurii.kasatkin.mkbur.2025@lpnu.ua*

# DISTINCTION BETWEEN THE ELECTRONIC COMMUNICATION SYSTEM OF THE NETWORK AND THE ELECTRONIC INFORMATION SYSTEM IN THE CONTEXT OF ENSURING CYBERSECURITY OF ORGANIZATIONS

**Abstract.** In the current environment of digital transformation of organizations, the complexity and interdependence between electronic communication networks (ECN) and electronic information systems (ES) is increasing, which raises the risks of cyberattacks and breaches of confidentiality, integrity, and availability of data. Insufficient separation between these two levels of IT infrastructure creates conditions for the spread of threats within a single information space, particularly during attacks such as lateral movement or privilege escalation. The article proposes a methodology for multi-level separation of ECN and EIS as a key direction for improving the cyber resilience of organizations. The model is based on the principles of network segmentation, isolation of information domains, role-based access control (RBAC), and the concept of zero trust architecture. Analytical modeling of the impact of segmentation on security indicators, the probability of compromise of critical nodes, the average time to incident, and the attack surface was performed. The simulation results showed that the implementation of the segmentation model reduces the number of compromised nodes by 25-30%, reduces the probability of compromising critical areas by more than 20%, and increases the average time to compromise by almost 50%. The developed methodology can be used as a basis for forming information security policies in government and corporate structures, as well as for building integrated protection systems based on the principles of flexible segmentation and trust management.

**Keywords:** cybersecurity, electronic communication network, electronic information system, network segmentation, Zero Trust, service isolation, access management.

## REFERENCES

1. Kotha, N. R. (2020). Network segmentation as a defense mechanism for securing enterprise networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 11*(3), 3023–3030. https://doi.org/10.61841/turcomat.v11i3.14942
2. Bondhala, S. (2025). Modern defense paradigms: Zero Trust architecture, network segmentation, and micro-segmentation. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/CSEIT25112714
3. Shastri, M. (2025). Understanding Zero-Trust architecture for developing comprehensive cybersecurity protocols. *International Journal of Advanced Research in Cyber Security, 3*(1), 1–4.
4. Santoso, E. (2022). Comparative analysis of network segmentation strategies to counter targeted attacks in global e-commerce cloud infrastructures. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 6*(12), 1–6.
5. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security, 2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1
6. Kaur, P., & Singh, M. (2022). Network segmentation and micro-segmentation in enterprise security architecture. *International Journal of Computer Applications, 183*(47), 22–28. https://doi.org/10.5120/ijca2022922120

7. IBM Security. (2023). *Cost of a data breach report 2023.* IBM Corporation. https://www.ibm.com/reports/data-breach
8. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
9. Bishop, M. (2018). *Introduction to computer security.* Addison-Wesley. ISBN 978-0-321-24744-2
10. Kurose, J., & Ross, K. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
11. International Organization for Standardization. (2018). *ISO/IEC 27000:2018 — Information security management systems — Overview and vocabulary.* Geneva.
12. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security, 2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1
13. Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *VDE Kongress.* Berlin.
14. Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS)* (pp. 1–7). https://doi.org/10.1109/SDN4FNS.2013.6702553
15. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
16. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST SP 800-145). https://doi.org/10.6028/NIST.SP.800-145
17. International Organization for Standardization. (2015). *ISO/IEC 27033-1:2015 — Network security — Part 1: Overview and concepts.* Geneva.
18. Sedgewick, M. (2021). Challenges in implementing Zero Trust networks. *IEEE Security & Privacy, 19*(3), 72–79. https://doi.org/10.1109/MSEC.2021.3062045
19. Hu, J., & Liu, H. (2022). Dynamic network segmentation for adaptive cyber defense. *Computers & Security, 116*, 102677. https://doi.org/10.1016/j.cose.2022.102677
20. Chandia, R., et al. (2009). Security strategies for SCADA networks. *International Journal of Critical Infrastructure Protection, 2*(1–2), 28–37. https://doi.org/10.1016/j.ijcip.2009.01.002
21. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust architecture.* https://doi.org/10.6028/NIST.SP.800-207
22. International Organization for Standardization. (2015). *ISO/IEC 27033-1:2015 — Network security — Part 1: Overview and concepts.* Geneva.
23. National Institute of Standards and Technology. (2011). *NIST SP 800-137: Information security continuous monitoring (ISCM) for federal information systems and organizations.* https://doi.org/10.6028/NIST.SP.800-137
24. Kreibich, T., & Crowcroft, J. (2023). Network topology and data flow mapping for cybersecurity. *Computers & Security, 117*, 102747. https://doi.org/10.1016/j.cose.2023.102747
25. Cisco Systems. (2022). *Network segmentation design guide* (White Paper). https://bookstation.org/book/cisco-ise-design-guide-4987197
26. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva.
27. Kindervag, J. (2010). *Building a Zero Trust network.* Forrester Research.
28. National Institute of Standards and Technology. (2014). *NIST SP 800-162: Guide to attribute-based access control (ABAC) definition and considerations.* https://doi.org/10.6028/NIST.SP.800-162
29. European Union Agency for Cybersecurity. (2023). *Access control in digital environments: Principles and best practices.*
30. European Union Agency for Cybersecurity. (2023). *Threat landscape 2023 — Main trends and emerging threats.*
31. Microsoft Security Architecture Center. (2023). *Zero Trust implementation guidance.* https://learn.microsoft.com/security/zero-trust
32. National Institute of Standards and Technology. (2014). *NIST SP 800-162: Guide to attribute-based access control (ABAC).* https://doi.org/10.6028/NIST.SP.800-162
33. Splunk Inc. (2023). *Security information and event management best practices.* https://www.splunk.com
34. Peterson, R. S. (2019). Unidirectional gateway security models. *IEEE Security & Privacy, 17*(4), 73–80. https://doi.org/10.1109/MSEC.2019.2914368
35. Noor, M., & Hassan, A. (2022). A survey on detection and prevention techniques for lateral movement in enterprise networks. *Computers & Security, 121*, 102859. https://doi.org/10.1016/j.cose.2022.102859
36. IBM Security. (2023). *Cost of a data breach report 2023.* https://www.ibm.com/reports/data-breach

37. CyberArk. (2023). *Privileged access management explained* (White Paper). https://www.cyberark.com/resources
38. OWASP Foundation. (2023). *API Security Top-10 2023.* https://owasp.org/API-Security
39. European Union Agency for Cybersecurity. (2023). *Threat landscape 2023 — Main trends and emerging threats.*