КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1017
УДК 004.056

Адаменко Володимир Олексійович,
старший викладач,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: 0000-0003-0601-8394
v.adamenko@kpi.ua

Козлов Дмитро Євгенович
PhD з комп'ютерної інженерії,
старший виклад кафедри інформаційних систем та технологій,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0007-1454-9036
d.kozlov@duikt.edu.ua

Коротков Сергій Станіславович
PhD з комп'ютерної інженерії, доцент,
доцент кафедри комп'ютерної інженерії
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4090-5934
s.korotkov@duikt.edu.ua

Миколаєнко Владислав Олександрович
асистент кафедри інформаційних систем та технологій,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0001-3384-3763
mykolaienkovlad@gmail.com

КОМПЛЕКСНІ ПІДХОДИ ДО ЗАХИСТУ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

Анотація. У статті представлено комплексне дослідження та обґрунтування стратегії ешелонованого захисту "Defense in Depth" як фундаментального підходу до забезпечення кібербезпеки сучасних корпоративних мереж. В основі цієї стратегії лежить припущення, що жоден окремий компонент захисту не є абсолютним, враховуючи потенційні вразливості, можливість обходу політик та непередбачуваний людський фактор. Дослідження детально аналізує ключові переваги ешелонованого захисту. Використовуючи статистичні дані, ща наведені у звітах IBM, Verizon та ін, було доведено, що ешелонований захист забезпечує надмірність, де відмова одного компонента компенсується іншими, створюючи мультиплікативний ефект блокування Такий підхід значно підвищує складність та вартість атаки для зловмисників на 40-60% порівняно з однорівневими системами. Запропонована в статті модель структурує захист на трьох взаємопов'язаних рівнях: технологічному, адміністративному та людському. Технологічний рівень розглядається як інструментальний фундамент, що включає три зони: захист периметра та мережі, захист кінцевих точок, та захист даних. Адміністративний рівень визначає організаційну та нормативну основу. Він включає політики безпеки, управління ідентифікацією та доступом з принципом найменших привілеїв та багатофакторною автентифікацією, а також моніторинг та аудит. Людський рівень аналізує людський фактор, який є причиною 74% витоків даних. У статті доводиться, що за системного підходу цей вразливий елемент перетворюється на ефективний "людський файрвол. Все це дозволяє зробити висновок, що лише комплексне поєднання технологічних, адміністративних та людських заходів в рамках єдиної стратегії "Defense in Depth" здатне забезпечити стійкий та економічно обґрунтований захист корпоративних мереж в умовах сучасних кіберзагроз.

Ключові слова: кібербезпека; корпоративна мережа; захист в глибину; ешелонований захист; siem; ngfw; edr; політика безпеки, людський фактор, культура безпеки.

ВСТУП

В епоху тотальної цифровізації, коли бізнес-процеси дедалі більше залежать від інформаційних технологій, а дані стають ключовим активом, забезпечення надійного захисту корпоративних мереж набуває першочергового значення. Стрімкий ріст кількості та складності кібератак, від фінансово мотивованих до атак на державні інституції, створює безпрецедентні ризики для організацій будь-якого масштабу. Ігнорування цих загроз може призвести не лише до фінансових втрат, але й до репутаційної шкоди, втрати довіри клієнтів та повної зупинки діяльності. Тому дослідження та впровадження комплексних, багаторівневих підходів до кібербезпеки є не просто технічним завданням, а критично важливою умовою для стабільного та успішного функціонування сучасного бізнесу.

Постановка проблеми. Сучасний ландшафт кіберзагроз характеризується високою динамічністю та складністю, що створює низку серйозних викликів для корпоративних систем безпеки. По-перше, масовий перехід на віддалені та гібридні формати роботи значно розширив периметр захисту, оголивши вразливості віддаленого доступу та створивши нові вектори для атак. По-друге, зловмисники використовують усе більш витончені інструменти, такі як цільові довготривалі атаки, що здатні непомітно перебувати в мережі місяцями, та руйнівні програми-вимагачі, які можуть паралізувати всю інфраструктуру компанії. По-третє, незмінним залишається ризик людського фактора: помилки співробітників, недостатня обізнаність у питаннях кібергігієни та успішні фішингові атаки часто стають початковою точкою для наймасштабніших інцидентів безпеки.

Аналіз останніх досліджень і публікацій. Сучасна наукова література пропонує глибокий аналіз численних інструментів та методологій для захисту комп'ютерних мереж. Значна частина досліджень зосереджена як на фундаментальних технологіях, так і на прикладних аспектах їх реалізації.

Наприклад, детально вивчені питання побудови захищених локальних та глобальних мереж, зокрема з використанням обладнання конкретних виробників. У цих роботах аналізуються технології захисту на канальному та мережевому рівнях, конфігурування VPN та політик безпеки на базі обладнання Cisco [1], [2].

Паралельно, велика увага приділяється новим викликам безпеки, що виникають у специфічних та стрімко зростаючих середовищах. Активно досліджуються проблеми підвищення рівня захисту в каналах передачі даних систем Інтернету речей (IoT) та розглядаються механізми забезпечення безпеки у децентралізованих пірингових (P2P) мережах [3], [4], які мають унікальні вектори атак.

Іншим потужним науковим напрямком є методологія оцінки ризиків мережевої безпеки. Дослідження в цій галузі еволюціонували від огляду та систематизації існуючих підходів до розробки нових, загальних методів оцінювання ризиків [5], [6]. Ці методи вдосконалюються для застосування у складних сценаріях, наприклад, для оцінки ризиків з точки зору цілісного «технологічного ланцюга» [7].

Однак, попри глибоке вивчення окремих технологій (Cisco) та специфічних доменів (IoT, P2P), а також наявність пропрацьованих методів оцінки ризиків, у науковій спільноті спостерігається брак робіт, що пропонують цілісну, інтегровану методологію саме для комплексного захисту корпоративної мережі.

Більшість публікацій розглядають окремі аспекти — чи то захист периметра [2], чи то оцінку ризиків — відносно ізольовано. Таким чином, виникає розрив між глибоким розумінням окремих загроз та практичною потребою в побудові єдиної, багаторівневої системи оборони.

Саме тому дослідження, спрямовані на розробку та обґрунтування єдиного методу комплексного захисту корпоративної мережі, який би об'єднував існуючі засоби та спеціалізовані механізми в синергетичну, ешелоновану систему, є особливо актуальними та науково значущими [8]-[11].

Метою цієї статті є дослідження комплексного підходу до захисту сучасних корпоративних мереж, що базується на синергії трьох фундаментальних рівнів: «Технології – Політики – Люди».

Стаття спрямована на вирішення таких завдань:

1. Проаналізувати ключові технологічні засоби захисту, що складають сучасний ешелонований кіберзахист.
2. Визначити роль організаційних політик, стандартів та процедур як основи для послідовного й ефективного управління безпекою.
3. Обґрунтувати критичну важливість людського фактора та запропонувати методи підвищення обізнаності й кібергігієни персоналу.

На відміну від вузькоспеціалізованих досліджень, що фокусуються лише на одному аспекті, дана стаття має на меті представити цілісну модель, яка дозволяє розглядати кібербезпеку не як суто технічне завдання, а як інтегрований бізнес-процес, де успіх залежить від гармонійного поєднання надійних інструментів, чітких правил та компетентних співробітників.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Концепція ешелонованого захисту (Defense in Depth). Концепція ешелонованого захисту, відома також як "захист у глибину", є стратегічним підходом до побудови систем інформаційної безпеки. Цей підхід відмовляється від ідеї єдиного, монолітного "периметра" на користь створення комплексної, багаторівневої системи оборони. В основі цієї стратегії лежить припущення, що жоден окремий компонент захисту не може гарантувати абсолютної надійності, оскільки будь-яка технологія потенційно містить вразливості, політики можуть бути обійдені, а людський фактор залишається джерелом ризику.

Рис. 1. Схематичне зображення концепції "Defense in Depth"

Таким чином, створюється система з кількох взаємодоповнюючих рівнів безпеки, де кожен ешелон призначений для стримування, затримки або виявлення атаки, якщо попередній рівень захисту був скомпрометований.

Ключовими перевагами ешелонованого захисту є:

- Надмірність та сукупна ефективність у разі відмови одного компонента, інші продовжують діяти. Це має мультиплікативний ефект: наприклад, якщо брандмауер блокує 90% шкідливого трафіку, а система IPS/IDS — 50% того, що пройшов, то сукупний рівень блокування вже становить 95% (а не 40%). Додавання EDR, яке блокує 99% решти загроз, доводить загальну ефективність до 99,95%, перетворюючи катастрофічний ризик на керований.
- Підвищення складності та вартості атаки кожен рівень вимагає від зловмисника унікальних інструментів та експлойтів. За експериментальними оцінками, вартість злому компанії з одним рівнем захисту (наприклад, лише антивірус) може бути в 10-20 разів нижчою, ніж атака на компанію з повноцінною ешелонованою обороною (NGFW + EDR + SIEM), оскільки остання вимагає значно більше часу та вищої кваліфікації.
- Скорочення часу виявлення (Dwell Time) проходження зловмисника через кілька рівнів генерує більше подій. Це дозволяє SIEM-системі швидше виявити аномалію. Згідно зі звітом IBM "Cost of a Data Breach 2023"[12], середній час виявлення інциденту становить 204 дні. Однак організації, що ефективно використовують інструменти AI та автоматизації (які є частиною зрілої багаторівневої системи), скорочують цей показник у середньому на 74 дні.
- Скорочення часу локалізації та реагування навіть після виявлення, локалізація загрози займає час (в середньому 73 дні). Багаторівневий захист (зокрема, сегментація мережі та EDR) дозволяє ізолювати скомпрометовані системи миттєво. Згідно з тим же звітом IBM[12], компанії з високим рівнем автоматизації та AI в безпеці скорочують життєвий цикл атаки (від виявлення до локалізації) в середньому на 108 днів порівняно з тими, хто їх не використовує.
- Пряме зниження фінансових збитків є прямим наслідком попередніх пунктів. Згідно з даними IBM, середня вартість витоку даних для компаній з низьким рівнем зрілості безпеки (без ешелонованого захисту) становить $5.09 мільйона. Для компаній з високим рівнем зрілості (що впровадили "Defense in Depth") ця цифра в середньому на $1.76 мільйона нижча і становить $3.33 мільйона.

2. Технологічний рівень захисту. Технологічний рівень, рис. 2, становить інструментальний та економічно обґрунтований фундамент всієї стратегії ешелонованого захисту, що є критично важливим. Цей рівень об'єднує комплекс апаратних і програмних засобів для блокування, виявлення та реагування на кіберзагрози, структуруючи їх за трьома основними зонами оборони. Перша зона, периметр і мережа, слугує зовнішнім бар'єром, де NGFW (Next-Generation Firewalls) та IPS демонструють ефективність блокування загроз вище 99.8%[13], а мережева сегментація стає ключовим інструментом протидії латеральному переміщенню — техніці, яку зловмисники здатні застосувати в середньому всього за 27-48 хвилин після початкового проникнення [14]. Друга зона, кінцеві точки, захищає безпосередні цілі атак за допомогою EDR (Endpoint Detection and Response); необхідність цього диктується тим, що кінцеві пристрої є мішенню для 16% атак (через фішинг) та потерпають від стрімкого зростання (на 58%) інфостілерів[15].

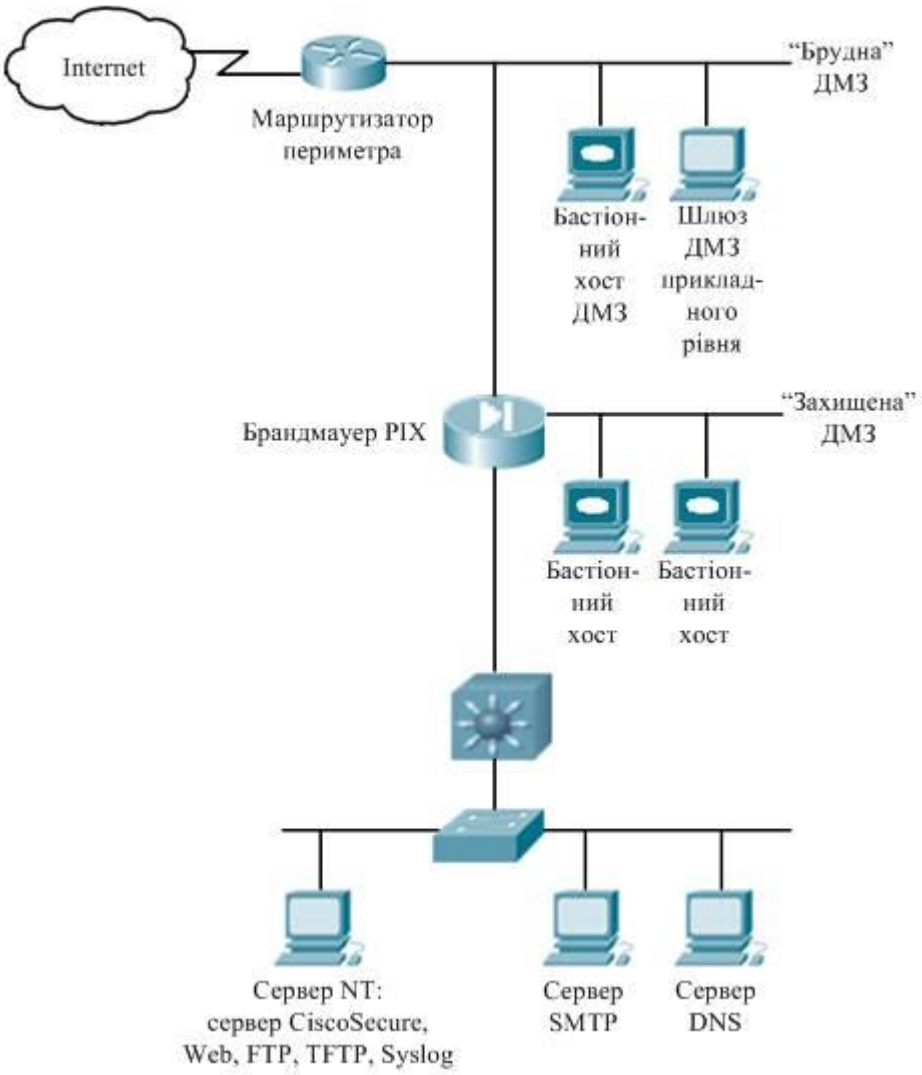

Рис. 2. Архітектурна схема мережі з елементами технологічного захисту.

2.1. Захист периметра та мережі. Цей ешелон контролює мережевий трафік на межі корпоративної мережі та всередині неї. Міжмережеві екрани (Firewalls) функціонують як бар'єр, аналізуючи трафік на основі правил і блокуючи неавторизовані з'єднання. Сучасні рішення (Next-Generation Firewalls, NGFW) забезпечують глибинну інспекцію пакетів (DPI), ідентифікуючи програми, користувачів та потенційні загрози.

Системи виявлення та запобігання вторгненням (IDS/IPS) здійснюють моніторинг. IDS (Intrusion Detection System) пасивно відстежує трафік для виявлення підозрілої активності, а IPS (Intrusion Prevention System) активно блокує шкідливий трафік у реальному часі.

Віртуальні приватні мережі (VPN) створюють захищений зашифрований канал через публічні мережі, забезпечуючи конфіденційність даних під час віддаленого доступу.

Сегментація мережі розділяє єдину мережу на ізольовані логічні підмережі. Цей підхід обмежує горизонтальне переміщення зловмисника, зменшуючи поверхню атаки та локалізуючи інциденти.

2.2. Захист кінцевих точок. Кінцеві точки (комп'ютери, сервери, мобільні пристрої) є основною ціллю атак. Платформи захисту кінцевих точок (EPP/EDR) допомагають убезпечити їх. EPP (Endpoint Protection Platform) — це еволюція антивірусного ПЗ, що використовує сигнатурні та поведінкові методи. EDR (Endpoint Detection and Response) забезпечує безперервний моніторинг і збір даних для виявлення складних загроз.

Контроль пристроїв (Device Control) дає можливість централізовано керувати використанням периферійних пристроїв, щоб запобігти витоку даних і поширенню шкідливого ПЗ.

2.3. Захист даних. Це останній рубіж оборони, спрямований на забезпечення конфіденційності та цілісності інформації. Шифрування (Encryption) — це криптографічне перетворення даних у нечитабельний формат. Воно застосовується як до даних «у спокої» (на носіях), так і до даних «у русі» (що передаються мережею).

Системи запобігання витокам даних (DLP) аналізують вміст даних у різних каналах комунікацій і на основі заданих політик блокують спроби несанкціонованої передачі конфіденційної інформації.

3. Адміністративний рівень захисту. Адміністративний рівень визначає організаційну та нормативну основу системи безпеки, перетворюючи технологічні інструменти на керовану бізнес-функцію. Він складається з політик, процедур та стандартів, що регламентують використання технологій та поведінку персоналу, і його вплив є прямо вимірюваним. Наприклад, процедури управління ідентифікацією та доступом (IAM) та політика найменших привілеїв є критичними, оскільки, за даними Verizon [16], 74% усіх витоків даних пов'язані з людським фактором, включно з крадіжкою облікових даних та зловживанням привілеями. Ефективність цього рівня також вимірюється через готовність до інцидентів, які мають сформовану та кваліфіковану команду реагування на інциденти (IR Team) — що є суто адміністративною функцією — економлять в середньому $1.49 мільйона під час витоку даних порівняно з тими, хто її не має. І навпаки, ігнорування стандартів (compliance) веде до фінансових втрат, а саме вартість витоку для компаній з високим рівнем невідповідності регуляціям є на 12.6% вищою ($5.05 млн) за середній показник.

3.1. Політики та процедури. Основою цього рівня є Політика інформаційної безпеки — документ верхнього рівня, який формалізує цілі, завдання та відповідальність організації у сфері захисту інформації. Він слугує нормативним фундаментом для розробки більш деталізованих стандартів, регламентів та інструкцій, встановлює рамки прийнятного використання ресурсів та є критерієм для проведення аудитів.

3.2. Управління ідентифікацією та доступом (IAM). IAM (Identity and Access Management) — це сукупність процесів та технологій для управління життєвим циклом облікових записів та їхніми правами доступу. Ключовими елементами IAM є: принцип найменших привілеїв (Principle of Least Privilege) - фундаментальна концепція, згідно з якою користувачам, системам та процесам надається мінімально необхідний рівень доступу та повноважень для виконання їхніх функціональних завдань. Це значно обмежує потенційну шкоду від скомпрометованого облікового запису; багатофакторна автентифікація (MFA): Метод верифікації ідентичності, що вимагає від користувача надання двох або більше доказів (факторів) для отримання доступу. MFA нівелює ризик несанкціонованого доступу внаслідок компрометації пароля. Фактори автентифікації поділяються на:

- Фактори знання (пароль, PIN-код).
- Фактори володіння (фізичний токен, смартфон з автентифікатором).

• Біометричні фактори (відбиток пальця, сканування обличчя).

3.3. Моніторинг та аудит. Цей компонент забезпечує постійний контроль за станом системи безпеки та відповідністю встановленим вимогам.

Системи SIEM (Security Information and Event Management): Централізовані платформи для агрегації, кореляції та аналізу журналів подій з різноманітних джерел (мережеве обладнання, сервери, застосунки). SIEM-системи дозволяють виявляти складні атаки та аномалії в реальному часі, які неможливо ідентифікувати на рівні окремих компонентів.

Регулярні аудити безпеки: Систематичні перевірки (внутрішні або зовнішні) для оцінки відповідності налаштувань політикам, виявлення вразливостей та контролю за дотриманням нормативних вимог. Аудити можуть включати сканування вразливостей, тестування на проникнення (penetration testing) та аналіз конфігурацій.

4. Людський рівень захисту. Людський фактор традиційно вважається однією з найбільш вразливих ланок у системі кібербезпеки, що підтверджується безапеляційною статистикою: згідно зі звітом Verizon DBIR[16] за 2024 рік, 74% усіх витоків даних так чи інакше пов'язані з людським фактором, включно з помилками, зловживанням привілеями, соціальною інженерією та фішингом. При цьому фішинг залишається однією з головних проблем, спричиняючи 16% усіх інцидентів. Однак, за умови правильного та системного підходу, людський фактор перетворюється на один з найефективніших рівнів захисту, що називають людський файрвой, рис.3.

Дослідження ефективності програм навчання (Security Awareness Training) показують, що організації, які впроваджують регулярні тренінги та контрольовані симуляції фішингових атак, здатні знизити відсоток співробітників, що "попадаються" на гачок, з початкового рівня 30-40% до менш ніж 5% протягом 12 місяців. Таким чином, інвестиції в персонал перетворюють найбільш непередбачуваний елемент системи з джерела ризику вартістю мільйони доларів на проактивний сенсор виявлення загроз.

Рис. 3: Піраміда зрілості людського рівня захисту.

4.1. Навчання та підвищення обізнаності (Security Awareness). Ключовим компонентом є програми підвищення обізнаності, спрямовані на регулярне інформування співробітників про актуальні загрози (фішинг, соціальна інженерія) та правила безпечної поведінки (парольна гігієна, поводження з конфіденційними даними). Ефективне навчання має бути безперервним процесом, а не одноразовим заходом.

4.2. Симуляція фішингових атак. Це практичний інструмент для оцінки та тренування персоналу. Проведення контрольованих симуляцій дозволяє об'єктивно виміряти рівень вразливості організації до фішингу та надати адресну допомогу тим

співробітникам, які продемонстрували ризиковану поведінку, перетворюючи їхні помилки на навчальний досвід у безпечному середовищі.

4.3. Формування культури безпеки. Стратегічною метою є інтеграція принципів кібербезпеки у корпоративні цінності та щоденні робочі процеси. Сильна культура безпеки характеризується проактивністю співробітників у виявленні загроз, підтримкою з боку керівництва та створенням атмосфери, в якій повідомлення про помилки чи інциденти заохочується з метою аналізу та вдосконалення, а не для покарання. Формування такої культури перетворює організацію на єдиний, стійкий до атак організм.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході дослідження було проаналізовано сучасні підходи до захисту корпоративних мереж та обґрунтовано переваги запропонованої комплексної моделі.

Традиційні підходи до кібербезпеки, що спираються на монолітний захист периметра або на використання окремих, не пов’язаних між собою технологічних рішень, демонструють свою неспроможність перед обличчям складних, багатоетапних атак. Такі підходи створюють хибне відчуття безпеки, адже компрометація єдиного рівня захисту призводить до повного доступу зловмисника до внутрішньої інфраструктури.

Запропонований у цій роботі підхід є значно ефективнішим, оскільки він базується на стратегії ешелонованого захисту "Defense in Depth", яка інтегрує три ключові рівні в єдину, синергетичну систему: технологічний, адміністративний та людський.

Переваги нашого підходу порівняно з існуючими полягають у наступному:

1. На відміну від розрізнених інструментів, наша модель забезпечує мультиплікативний ефект, де кожен наступний ешелон блокує загрози, пропущені попереднім. Це перетворює катастрофічні ризики на керовані, доводячи сукупну ефективність блокування до 99,95% і підвищуючи вартість атаки для зловмисника в 10-20 разів.
2. Існуючі рішення часто ігнорують людський рівень або розглядають його виключно як слабку ланку, джерело 74% інцидентів. Запропонований підхід доводить, що системні інвестиції в навчання, симуляції фішингу та формування культури безпеки перетворюють персонал на "людський файрвол". Це проактивний сенсор, здатний знизити вразливість до фішингу з 30-40% до менш ніж 5%.
3. Вимірювана економічна ефективність. Запропонована модель має прямий та вимірюваний фінансовий вплив. Впровадження зрілої ешелонованої системи, що включає адміністративний контроль та технологічну автоматизацію, безпосередньо знижує середню вартість витоку даних на $1.76 мільйона та скорочує загальний життєвий цикл атаки: виявлення та локалізація, на 108 днів.
4. На відміну від суто технологічних підходів, запропонований підхід є стійким до збоїв. Він поєднує інструменти, правила та навички. Навіть якщо технологія дасть збій або політика буде обійдена, навчений персонал та коректні налаштування доступу слугуватимуть ефективними бар'єрами, що локалізують інцидент .

Таким чином, представлений комплексний підхід, що поєднує технологічний, адміністративний та людський рівні захисту, значно підвищує складність та вартість атаки для зловмисників в середньому на 40-60% порівняно з однорівневими системами Він створює не просто набір бар'єрів, а стійку, глибоко інтегровану та економічно обґрунтовану систему безпеки, здатну адаптуватися до загроз та перетворювати найвразливіші елементи на ефективні засоби захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zakharchenko, S. M., Troianovska, T. I., & Boiko, O. V. (2017). *Building secure networks based on Cisco equipment*. [Textbook]. Vinnytsia: VNTU. 133 p.
2. Korobeinikova, T. I., & Zakharchenko, S. M. (2021). *Local network protection technologies based on CISCO equipment*. [Textbook]. Lviv: Lviv Polytechnic Publishing House. 188 p.
3. Korobeinikova, T. I., & Zakharchenko, S. M. (2022). *Computer networks*. [Textbook]. Lviv: Lviv Polytechnic Publishing House. 228 p.
4. Gorokhovskyi, O. I., & Troianovska, T. I. (2007). *Modeling, creation and practice of automated distance learning systems*. Information technologies and computer engineering, 1(8), 235–239.
5. Gorokhovskyi, O. I., Troianovska, T. I., & Azarov, O. D. (2016). *Information technology of content delivery in systems of computerized training of specialists*. [Monograph]. Vinnytsia: VNTU. 160 p.
6. Malinovskyi, V. I., Kupershtein, L. M., Lukichov, V. V., & Dudatiev, A. V. (2024). *Problems and approaches to increasing the level of protection in data transmission channels of IoT systems and devices*. Visnyk of Vinnytsia Polytechnic Institute, (4), 105–115. https://doi.org/10.31649/1997-9266-2024-175-4-104-114
7. Luzhetskyi, V., & Savytska, L. (2024). *Data protection mechanisms in peer-to-peer networks*. Herald of Khmelnytskyi National University. Technical sciences, 339(4), 503–508. https://doi.org/10.31891/2307-5732-2024-339-4-74
8. Chynchyk, D. M., Korobeinikova, T. I., & Zakharchenko, S. M. (2021). *Methods and means of comprehensive corporate network protection*. Scientific Collection «InterConf», (84), 433–450. Rome, Italy: Dana. https://doi.org/10.51582/interconf.7-8.11.2021.043
9. Chynchyk, D. M., & Korobeinikova, T. I. (2023). *Methods and means of comprehensive corporate network protection*. Strategic directions of science development: factors of influence and interaction: Proceedings of the II International Scientific Conference (pp. 97–102). Vinnytsia: European Scientific Platform.
10. Chynchyk, D., Korobeinikova, T., & Luzhetska, N. (2023). *Method of comprehensive corporate network protection*. Information protection and information systems security: Materials of IX International Scientific and Technical Conference (pp. 29–30). Lviv: Lviv Polytechnic Publishing House. https://doi.org/10.30890/2709-2313.2025-38-02-001
11. Chynchyk, D., & Korobeinikova, T. (2021). *Specialized mechanisms for protecting the corporate network in terms of network security*. Information protection and information systems security: Materials of VIII-th International Scientific and Technical Conference (pp. 51–53). [Textbook] Lviv: NULP.
12. IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf
13. CyberRatings. (2025). *Comparative Security Map 2025*. https://cyberratings.org/reports/security-service-edge-sse-threat-protection/
14. ReliaQuest. (2025). *2025 Annual Cyber-Threat Report*. https://reliaquest.com/campaigns/stay-ahead-of-evolving-risks/2025-annual-cyber-threat-report
15. Check Point. (2024). *2024 Cyber Security Report*. https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a
16. Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

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

Adamenko Volodymyr
Senior Lecturer,
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0003-0601-8394
v.adamenko@kpi.ua

Dmytro Kozlov
PhD in Computer Engineering,
Senior Lecturer of the Department of Information Systems and Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0007-1454-9036
d.kozlov@duikt.edu.ua

Korotkov Serhii
PhD in Computer Engineering, Associate Professor,
Associate Professor of the Department of Computer Engineering
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4090-5934
s.korotkov@duikt.edu.ua

Mykolaienko Vladyslav
Assistant professor of the Department of Information Systems and Technologies,
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0001-3384-3763
mykolaienkovlad@gmail.com

COMPREHENSIVE APPROACHES TO THE PROTECTION OF MODERN CORPORATE NETWORKS

Abstract. The article presents a comprehensive study and substantiation of the "Defense in Depth" strategy as a fundamental approach to ensuring the cybersecurity of modern corporate networks. At the core of this strategy lies the assumption that no single defense component is absolute, considering potential vulnerabilities, the possibility of policy bypass, and the unpredictable human factor. The research analyzes in detail the key advantages of layered defense. Using statistical data cited in reports from IBM, Verizon, et al., it is demonstrated that layered defense provides redundancy, where the failure of one component is compensated by others, creating a multiplicative blocking effect. This approach significantly increases the complexity and cost of an attack for malicious actors by 40-60% compared to single-layer systems. The model proposed in the article structures defense on three interconnected levels: technological, administrative, and human. The technological level is considered the instrumental foundation, which includes three zones: perimeter and network protection, endpoint protection, and data protection. The administrative level defines the organizational and regulatory framework. It includes security policies, identity and access management (IAM) with the principle of least privilege and multi-factor authentication, as well as monitoring and auditing. The human level analyzes the human factor, which is the cause of 74% of data breaches. The article argues that with a systematic approach, this vulnerable element is transformed into an effective "human firewall." All this leads to the conclusion that only a comprehensive combination of technological, administrative, and human measures within a unified "Defense in Depth" strategy can provide sustainable and cost-effective protection for corporate networks against modern cyber threats.

Keywords: cybersecurity; corporate network; defense in depth; layered defense; siem; ngfw; edr; security policy; human factor; security culture.

REFERENCES

1. Zakharchenko, S. M., Troianovska, T. I., & Boiko, O. V. (2017). *Building secure networks based on Cisco equipment*. [Textbook]. Vinnytsia: VNTU. 133 p.
2. Korobeinikova, T. I., & Zakharchenko, S. M. (2021). *Local network protection technologies based on CISCO equipment*. [Textbook]. Lviv: Lviv Polytechnic Publishing House. 188 p.
3. Korobeinikova, T. I., & Zakharchenko, S. M. (2022). *Computer networks*. [Textbook]. Lviv: Lviv Polytechnic Publishing House. 228 p.
4. Gorokhovskyi, O. I., & Troianovska, T. I. (2007). *Modeling, creation and practice of automated distance learning systems*. Information technologies and computer engineering, 1(8), 235–239.
5. Gorokhovskyi, O. I., Troianovska, T. I., & Azarov, O. D. (2016). *Information technology of content delivery in systems of computerized training of specialists*. [Monograph]. Vinnytsia: VNTU. 160 p.
6. Malinovskyi, V. I., Kupershtein, L. M., Lukichov, V. V., & Dudatiev, A. V. (2024). *Problems and approaches to increasing the level of protection in data transmission channels of IoT systems and devices*. Visnyk of Vinnytsia Polytechnic Institute, (4), 105–115. https://doi.org/10.31649/1997-9266-2024-175-4-104-114
7. Luzhetskyi, V., & Savytska, L. (2024). *Data protection mechanisms in peer-to-peer networks*. Herald of Khmelnytskyi National University. Technical sciences, 339(4), 503–508. https://doi.org/10.31891/2307-5732-2024-339-4-74
8. Chynchyk, D. M., Korobeinikova, T. I., & Zakharchenko, S. M. (2021). *Methods and means of comprehensive corporate network protection*. Scientific Collection «InterConf», (84), 433–450. Rome, Italy: Dana. https://doi.org/10.51582/interconf.7-8.11.2021.043
9. Chynchyk, D. M., & Korobeinikova, T. I. (2023). *Methods and means of comprehensive corporate network protection*. Strategic directions of science development: factors of influence and interaction: Proceedings of the II International Scientific Conference (pp. 97–102). Vinnytsia: European Scientific Platform.
10. Chynchyk, D., Korobeinikova, T., & Luzhetska, N. (2023). *Method of comprehensive corporate network protection*. Information protection and information systems security: Materials of IX International Scientific and Technical Conference (pp. 29–30). Lviv: Lviv Polytechnic Publishing House. https://doi.org/10.30890/2709-2313.2025-38-02-001
11. Chynchyk, D., & Korobeinikova, T. (2021). *Specialized mechanisms for protecting the corporate network in terms of network security*. Information protection and information systems security: Materials of VIII-th International Scientific and Technical Conference (pp. 51–53). [Textbook] Lviv: NULP.
12. IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf
13. CyberRatings. (2025). *Comparative Security Map 2025*. https://cyberratings.org/reports/security-service-edge-sse-threat-protection/
14. ReliaQuest. (2025). *2025 Annual Cyber-Threat Report*. https://reliaquest.com/campaigns/stay-ahead-of-evolving-risks/2025-annual-cyber-threat-report
15. Check Point. (2024). *2024 Cyber Security Report*. https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a
16. Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf