УДК 004.05 **DOI:10.30837/rt.2025.3.222.02**

В.В. БОРОДАВКА, В.І. ЄСІН, д-р техн. наук

ВПРОВАДЖЕННЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ НА ОСНОВІ ЗАПРОПОНОВАНОЇ МОДЕЛІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Вступ

В умовах стрімкої цифрової трансформації та зростання загроз у кіберпросторі актуальність питань організації кібербезпеки підприємств набуває особливої значущості. Зростаючий обсяг пристроїв, що підключаються до мережі, зокрема через технологію Інтернету речей (Internet of Things), швидкий розвиток нових технологій штучного інтелекту (ШІ), генеративного ШІ, квантових обчислень та постійне зростання складності кібератак створюють необхідність реалізації інноваційних підходів до забезпечення безпеки даних. Традиційні методи захисту на основі периметру виявляються неефективними перед сучасними кіберзагрозами. Відповіддю на ці виклики стала концепція нульової довіри, як один із найефективніших підходів для протидії сучасним кіберзагрозам. Вона ґрунтується на принципі «ніколи не довіряй, завжди перевіряй» і передбачає, що жоден користувач, пристрій або процес не повинен автоматично вважатися безпечним, навіть якщо вони знаходяться всередині корпоративної мережі.

Концепція нульової довіри була запропонована вперше S. P. Marsh у 1994 р. [1]. Проте значний крок у її розвитку відбувся лише в 2003 р., коли консорціум Jericho Forum представив концепцію [2], яка передбачала використання принципів нульової довіри як стратегії безпеки для деперіметризації (de-perimeterization), що фактично означало усунення межі між організацією та зовнішнім світом. У 2009 р. Google впровадив модель BeyondCorp [3], яка поклала початок застосуванню концепції нульової довіри у корпоративному середовищі. Дана модель передбачала автентифікацію на основі перевірки користувача та пристрою, що дозволяло відмовитися від привілейованих корпоративних мереж. У 2010 р. J. Kindervag (аналітик компанії Forrester) використав концепцію нульової довіри для контролю доступу [4]. Він наголосив, що традиційні методи безпеки є недостатніми для протидії сучасним кіберзагрозам. Саме тоді було сформульовано ключовий принцип концепції нульової довіри: «ніколи не довіряй, завжди перевіряй» [4]. Подальший розвиток концепції призвів до появи у 2017 р. розширеної концепції нульової довіри (Zero Trust Extended – ZTX) від компанії Forrester [5], що охоплювала ширше коло потоків даних, зокрема тих, що проходять через локальні мережі, хмарні сервіси, зовнішні застосунки, сайти та різні види кінцевих пристроїв. Компанія Gartner [6], ґрунтуючись на принципі безперервної адаптивної оцінки ризиків та довіри (Continuous Adaptive Risk and Trust Assessment – CARTA), також висунула ідею про ZTX. Надалі, додатковий імпульс розвитку концепції надали публікації NIST [7] та NCCoE (National Cybersecurity Center of Excellence) [8], які визначали основні принципи та компоненти нульової довіри, і акцентували увагу на архітектурі нульової довіри (Zero Trust Architecture – ZTA) для захисту корпоративних даних [9]. Подальший розвиток концепції нульової довіри відзначається інтеграцією системи виявлення та реагування на кіберзагрози в ZTA, включно із системами захисту кінцевих точок (Endpoint Detection and Response – EDR), розширеним виявленням та реагуванням (eXtended Detection and Response – XDR), а також мережевим виявленням та реагуванням (Network Detection and Response – NDR). Ці технології відіграють ключову роль у забезпеченні корпоративної безпеки, оскільки спрямовані на виявлення, аналіз і нейтралізацію атак, що здатні обходити традиційні засоби захисту, зокрема платформи захисту кінцевих пристроїв (Endpoint Protection Platform – EPP). Іншим важливим аспектом впровадження ZTA в умовах поширення гібридних робочих середовищ є забезпечення безпеки віддаленого доступу (Remote Access Security), що реалізується за допомогою багатофакторної автентифікації (Multifactor Authentication – MFA), політик

контролю доступу та наскрізного шифрування мережевого трафіку. Застосування ZTA є ефективним заходом протидії атакам на ланцюги постачання (Supply Chain Attacks), які дедалі частіше використовуються як вектор компрометації корпоративних мереж, що зумовлює необхідність обмеження доступу сторонніх постачальників до критично важливих систем та впровадження детального моніторингу їхньої активності з метою зниження ризику несанкціонованого втручання. Окремої уваги заслуговують атаки на відкриті програмні інтерфейси (Application Programming Interface – API), які можна використовувати для несанкціонованого доступу до корпоративних даних. В цьому контексті застосування шлюзів для автентифікації та мікросегментація дозволяє значно зменшити ризики, пов'язані з вразливостями API. Проте, окрім корпоративних мереж, ZTA має критичне значення для захисту промислових систем управління (Industrial Control Systems – ICS) та операційних технологій (Operational Technology). Дані системи є частиною критичної інфраструктури, які є постійними цілями для кібератак, в свою чергу ZTA може допомогти мінімізувати ризики кібератак на ці системи. Наприклад, під час атаки NotPetya у 2017 р. [10], яка завдала значних фінансових та операційних збитків підприємствам, впровадження принципів нульової довіри дозволило б обмежити поширення шкідливого програмного забезпечення (ПЗ) шляхом бічного переміщення (lateral movement) та мінімізувати його вплив на інфраструктуру. Водночас, ефективність реалізації ZTA значною мірою залежить від здатності системи своєчасно ідентифікувати загрози та реагувати на них. Зокрема, важливим аспектом є те, що успішна атака можлива навіть після численних невдалих спроб, тоді як захист повинен працювати безперебійно, запобігаючи будь-якій компрометації. У зв'язку з цим зростає необхідність впровадження механізмів, що забезпечують безперервний моніторинг трафіку, аналіз поведінки користувачів та пристроїв, а також адаптивне реагування на потенційні загрози. Оскільки ймовірність кібератаки неминуча, а абсолютний захист є лише теоретичним [11], ключовим завданням стає мінімізація ризиків шляхом раннього виявлення та миттєвого реагування.

На сьогодні концепція нульової довіри набуває все більшого поширення, її застосовують у різних сферах, від хмарних сервісів до 5G-мереж для медичних пристроїв [12]. За даними аналітичної компанії MarketsandMarkets [13] прогнозується, що ринок ZTA зросте від 36,5 мільярдів доларів США у 2024 р. до 78,7 мільярдів доларів у 2029 р., з середньорічним темпом зростання 16,6 % протягом даного періоду. Це свідчить про високу ефективність моделі нульової довіри у зменшенні ризиків від кібератак, підвищенні загальної безпеки інформаційних систем та про значне поширення ZTA як у вертикальному (різні галузі), так і у горизонтальному (різні регіони) вимірах. Таким чином, подальший розвиток і впровадження ZTA є важливим кроком у підвищенні загальної стійкості кібербезпеки підприємств, що дозволить створювати динамічні системи захисту, здатні не лише протистояти сучасним атакам, але й адаптуватися до нових викликів.

Виходячи з зазначеного, концепція нульової довіри є ключовим підходом до побудови сучасних систем кібербезпеки, що дозволяє значно підвищити рівень захищеності інформаційних ресурсів підприємства. Проте, попри очевидні переваги концепції нульової довіри, процес її впровадження в корпоративні інформаційні системи супроводжується значними труднощами як з технічної, так і з організаційної точки зору. Як видно з досліджень [14, 15], існує проблема, пов'язана з відсутністю підходу до впровадження ZTA, який враховував би як технічні, так і організаційні аспекти. Дана робота націлена на вирішення цієї проблеми шляхом узагальнення наявних досліджень та досвіду різних міжнародних компаній, а також розробки на основі цього моделі впровадження ZTA для організації кібербезпеки підприємства. Це дозволить підприємствам ефективно адаптувати підхід нульової довіри відповідно до своїх потреб та особливостей власної інфраструктури. У статті розглядаються рекомендації щодо вибору моделей розгортання ZTA для різного роду діяльності підприємств, а також модель впровадження ZTA, що допоможе зрозуміти фундаментальні зміни у підході до організації кібербезпеки, а також ефективно впровадити концепцію нульової довіри з урахуванням технічних та організаційних можливостей і вимог конкретного IT-підприємства.

1. Рекомендації щодо вибору моделей розгортання архітектури нульової довіри для різних підприємств

Захист корпоративних даних і ресурсів стає дедалі складнішим завданням. Багатьом користувачам потрібен доступ з будь-якого місця, в будь-який час, з будь-якого пристрою, для забезпечення функціональної діяльності організації. В свою чергу, дані створюються, зберігаються, передаються та обробляються в різних корпоративних мережах і розподілені між локальними та хмарними середовищами, щоб задовольнити потреби бізнесу, які постійно змінюються. Вже неможливо просто захистити дані та ресурси за периметром корпоративного середовища або припустити, що всім користувачам, пристроям, застосункам і сервісам в ньому можна довіряти.

ZTA є ефективним підходом до забезпечення кібербезпеки, який дозволяє організаціям захищати свої дані та ресурси незалежно від їхнього місцезнаходження. Концепція нульової довіри ґрунтується на ризик-орієнтованому підході до управління доступом, що передбачає постійний моніторинг, оцінку та перевірку умов і запитів на доступ із подальшим наданням або обмеженням доступу залежно від рівня ризику. Кожен запит на доступ у межах ZTA явно перевіряється з урахуванням контексту, що включає як статичну інформацію, так і динамічні фактори. Якщо запит відповідає визначеним політикам, створюється безпечний сеанс доступу до даних. ZTA також забезпечує безперервний моніторинг та оцінку ризиків у реальному часі, що дозволяє динамічно застосовувати корпоративні політики безпеки. Варто зазначити, оскільки впровадження ZTA є складним процесом, організації потребують структурованого підходу до її реалізації. Насамперед необхідно провести комплексну оцінку поточних ресурсів, визначити сильні та слабкі сторони існуючої інфраструктури, а також окреслити ключові етапи переходу до ZTA. Поетапне впровадження дозволяє поступово адаптувати корпоративне середовище до вимог ZTA, враховуючи наявні ризики, витрати, доступні ресурси та стратегічні пріоритети. Важливим аспектом цього процесу є забезпечення балансу між підвищенням рівня безпеки та збереженням ефективності бізнес-процесів. При цьому слід зазначити, що не існує універсального підходу до впровадження ZTA, який був би однаково ефективним для всіх підприємств. ZTA – це набір керівних принципів та концепцій, а не набір технічних специфікацій, яких можна дотримуватися. Тому впровадження ZTA передбачає не фіксований набір вимог, а безперервний процес удосконалення процесів, механізмів контролю доступу та політик безпеки відповідно до принципів ZTA та специфіки кожного підприємства.

Основними перевагами від впровадження концепції нульової довіри на підприємстві, як зазначається у роботах [9, 15, 16], є:

1. Поліпшення видимості мережі, виявлення зловживань або порушень та керування вразливостями (покращення видимості того, які користувачі, коли, як і звідки отримують доступ до тих чи інших ресурсів та які дії виконують).

2. Перешкода поширенню шкідливого ПЗ, а саме більш ефективне виявлення, реагування та відновлення після інцидентів, що дозволяє мінімізувати наслідки витоків даних, а також мінімізація ризику бічного переміщення.

3. Оптимізація та скорочення витрат, пов’язаних із забезпеченням безпеки, а також скорочення обсягу та вартості робіт, необхідних для дотримання та забезпечення нормативних вимог і стандартів безпеки.

4. Усунення конфліктів між підрозділами при розслідуванні інцидентів. Наприклад, у випадку деяких інцидентів мережеві спеціалісти можуть звинувачувати службу безпеки у створенні перешкод у роботі, тоді як служба безпеки може вказувати на недоліки в мережевій інфраструктурі. Концепція нульової довіри сприяє налагодженню взаємодії між робочими групами, дозволяючи усунути подібні протиріччя шляхом чіткої регламентації доступу та відповідальності.

5. Підвищення рівня обізнаності, розуміння та контролю даних.

6. Комплексний захист інформаційних ресурсів і критичних активів, що включає запобігання витоку важливих даних до зловмисників шляхом обмеження їх можливостей, зниження рівня внутрішніх загроз, застосування надійного шифрування для захисту важливих (sensitive) корпоративних даних як під час передачі, так і в стані спокою. Додатково передбачено динамічний контроль доступу з урахуванням ризиків шляхом постійного моніторингу активності, безперервної переоцінки всіх операцій та сеансів доступу, збору інформації, отриманої в результаті періодичної повторної автентифікації та авторизації користувачів, постійної оцінки стану пристроїв, аналізу поведінки, виявлення аномалій у режимі реального часу та інших аналітичних даних щодо безпеки. Наприклад, система може автоматично обмежити доступ до конфіденційних файлів, якщо користувач входить із незвичного місця або використовує потенційно скомпрометований пристрій.

7. Забезпечення цифрової трансформації бізнесу, що включає підтримку віддаленої роботи, надання працездатних пристроїв від постачальників, гнучке керування доступом для співробітників і підвищення якості обслуговування кінцевих користувачів.

Проте, під час впровадження ZTA можуть виникати деякі специфічні загрози [15], які мають унікальні особливості (наприклад, спотворення процесу прийняття рішень; відмова в обслуговуванні або порушення роботи мережі; крадіжка облікових даних (інсайдерська загроза); видимість у мережі; зберігання системної та мережевої інформації; залежність від пропрієтарних/власних форматів даних або рішень; використання сутностей, які не є фізичними особами, при адмініструванні ZTA), для яких також мають місце певні рішення у межах реалізації певної ZTA. При цьому слід розуміти, що при розгортанні рішень, які задовольняють вимогам концепції нульової довіри, як зазначається у роботах [17 – 23], організації можуть зіткнутися з численними технічними та організаційними викликами (табл. 1), які повинні враховуватися під час впровадження ZTA.

Таблиця 1

Виклики при розгортанні рішень на основі концепції нульової довіри

Організаційні	**Технічні**
✓ Помилкове розуміння, що ZTA підходить лише для великих організацій і вимагає значних інвестицій, замість розуміння того, що ZTA – це набір керівних принципів, придатних для організацій будь-якого розміру. ✓ Занепокоєння, що ZTA може негативно вплинути на функціонування IT-середовища або на роботу кінцевих користувачів. ✓ Недостатність ресурсів для розробки необхідних політик та експериментальної реалізації, необхідних для формування плану переходу до ZTA. ✓ Ефективне використання наявних ресурсів та баланс пріоритетів під час переходу до ZTA. ✓ Відсутність розуміння того, які додаткові навички та навчальні програми можуть знадобитися адміністраторам, співробітникам служби безпеки, постачальникам послуг, кінцевим користувачам. ✓ Недостатня розвиненість стандартизованих політик для впровадження, керування та забезпечення дотримання вимог ZTA, що призводить до фрагментованості середовища або несумісності окремих компонентів в рамках архітектури. ✓ Відсутність універсального підходу до реалізації та впровадження ZTA потребує розробки індивідуальних стратегій та політик впровадження, що враховують специфіку організаційних процесів, рівень прийнятного ризику, поточну технологічну базу та фінансові можливості.	✓ Відсутність належної системи інвентаризації та управління активами, необхідної для повного розуміння бізнес-інфраструктури, активів та процесів, які потребують захисту, а також відсутність чіткого розуміння критичності даних ресурсів. ✓ Відсутність або обмежене розуміння процесів, що відбуваються між суб'єктами, активами, застосунками та сервісами організації, а також відсутність даних, необхідних для ідентифікації цих процесів та їхніх конкретних потоків. ✓ Складність інтеграції різнорідних доступних технологій, оцінки їхньої відповідності вимогам ZTA, а також виявлення технологічних недоліків, що необхідні для формування комплексної ZTA. ✓ Проблеми сумісності ZTA із застарілими/успадкованими системами, що потребують додаткових ресурсів для адаптації або заміни. ✓ Відсутність належного цифрового опису, керування та контролю ролей користувачів в організації, необхідних для впровадження детальної політики доступу до певних застосунків та сервісів

Одним із ключових аспектів впровадження ZTA є необхідність поступового підходу, що дозволяє мінімізувати ризики та забезпечити адаптацію інфраструктури підприємства до нових умов. У цьому контексті першочерговим завданням є визначення стратегії переходу, яка відповідно до рекомендацій NIST [7], повинна містити поетапний підхід із впровадженням експериментального проєкту. На початковому етапі визначаються об'єкти та системи, які першочергово підлягають міграції, після чого процес поступово масштабується на інші компоненти інфраструктури. Крім того, акцент робиться на ідентифікації активів, бізнес-процесів і керуванні ризиками. В свою чергу, дослідження, проведені компанією Cisco [24], акцентують увагу на механізмах автентифікації, моніторингу користувачів та пристроїв, а також окреслюють три ключові аспекти впровадження ZTA: стратегічний, управлінський і операційний. Водночас у дослідженні недостатньо деталізовано методи та технічні аспекти міграції, що ускладнює практичну реалізацію ZTA. Прикладом технічного підходу до міграції є реалізація Google BeyondCorp [3, 25], де основна увага приділяється впровадженню керування користувачами, пристроями та мережевою інфраструктурою в рамках концепції нульової довіри. Міграція реалізується поетапно, з початковим тестуванням на обмеженій кількості систем, після чого проводиться аналіз ефективності та поступова інтеграція в масштабах усієї інфраструктури.

У свою чергу, підхід Microsoft [26] орієнтується на управлінські аспекти міграції, зокрема на визначення меж та етапів реалізації моделі нульової довіри. Згідно з цією стратегією, Microsoft структурно розподіляє впровадження ZTA на ключові компоненти, такі як ідентифікація користувачів, керування пристроями, доступ до ресурсів та сервісів, визначаючи критерії оцінки ефективності впровадження ZTA.

NCCoE [8] активно співпрацює з численними постачальниками технологій, наприклад, такими як AWS, Broadcom, Cisco, Google Cloud, IBM, Ivanti, Microsoft, Okta, Palo Alto Networks, Tenable, що дозволяє інтегрувати комерційні і відкриті рішення (open-source) та забезпечити комплексну безпеку згідно з принципами концепції нульової довіри. У рамках цього підходу багато досліджень [27 – 29] із впровадження ZTA визначають основні етапи, які необхідно пройти для забезпечення надійного захисту підприємства. Серед них першочерговим етапом є ідентифікація об'єктів захисту, що охоплюють дані, активи, застосунки та сервіси. Наступним кроком є визначення потоків даних, що взаємодіють із цими об'єктами, для забезпечення належного контролю доступу та запобігання несанкціонованому доступу до критичних ресурсів. Далі важливим є архітектурне проектування мережі, яке повинно враховувати принципи мікросегментації. Завершальним етапом є розробка та впровадження політики нульової довіри, що передбачає безперервну автентифікацію та авторизацію всіх запитів на доступ до ресурсів, незалежно від їхнього походження або місцезнаходження користувача чи сервісу, що дозволяє забезпечити безпечний та ефективний захист інфраструктури підприємства на всіх етапах її життєвого циклу.

Проте, попри широке визнання переваг ZTA, значна частина досліджень обмежується лише загальним описом основних етапів її впровадження, без детального обґрунтування підходів до міграції. Крім того, багато робіт зосереджуються на вузьких технічних або організаційних аспектах, ігноруючи динамічні та комплексні методи, що забезпечують поступовий і ефективний перехід до ZTA. На думку фахівців NIST, ZTA може різнитися залежно від потреб компанії. Для цього вони розглядають можливість застосування кількох різних підходів (шляхів), за допомогою яких підприємство може запровадити ZTA для робочих процесів, зокрема: вдосконалене/покращене управління ідентифікацією (enhanced identity governance), логічну мікросегментацію (logical micro-segmentation) та сегментацію на основі мережі (network-based segmentation) [7]. У роботі [15] докладно описані дані підходи та визначена різниця в них між компонентами, що використовуються, і основним джерелом правил політики для організації. При цьому варто зазначити, що одні підходи найбільше підходять для одних випадків, тоді як інші доцільно використовувати в інших ситуаціях. Тому підприємство, яке прагне розробити та впровадити ZTA, може виявити, що обраний ним варіант використання

та існуючі політики виділяють один підхід серед інших існуючих. Однак це не означає, що інші підходи не працюватимуть. Зважаючи на все, це лише вказує на те (і не більше), що інші підходи можуть бути більш важкими для реалізації і можуть вимагати кардинальніших змін в організації розвитку бізнесу.

З іншого боку, розглядати потенційні рішення з нульовою довірою доцільно з погляду їх моделей розгортання, які можуть бути корисною основою, за допомогою якої підприємства зможуть оцінити потенційних постачальників відповідних рішень, аналізуючи їх плюси та мінуси. Вважається, що багато з корпоративних моделей нульової довіри, що надаються постачальниками, будуть відповідати одній або декільком моделям розгортання. Наразі відомі такі поширені варіанти розгортання ZTA на підприємствах [7, 15, 30]:

1. Модель агента пристрою/шлюзу (Device Agent/Gateway Model; іноді цю модель називають моделлю розгортання на основі ресурсів – Resource-Based Deployment Model).

2. Модель розгортання з мікросегментацією (Micro-Segmentation Deployment Model).

3. Модель розгортання на основі анклаву (Resource Enclave Deployment Model).

4. Модель розгортання на основі порталу ресурсів (Resource Portal-Based Deployment).

5. Модель розгортання з використанням хмарної маршрутизації (Cloud-Routed Deployment Model).

6. Модель розгортання на основі використання «пісочниці» (sandboxing) застосунків.

Дані моделі можуть оцінити та надати новий рівень деталізації того, як насправді можуть бути розгорнуті системи з ZTA. Хоча при цьому не слід забувати, що реальна архітектура розгортання, звичайно ж, буде залежати від можливостей обраної технології [15] та може відбуватися з використанням декількох моделей залежно від особливостей підприємства та його технологічних можливостей. Варто зазначити, що будь-яке IT-середовище може бути спроектоване з урахуванням принципів нульової довіри, а більшість організацій вже мають певні елементи ZTA в своїй корпоративній інфраструктурі або знаходяться на шляху до впровадження політик і передових практик. З огляду на це, важливим аспектом є врахування різних сценаріїв при розгортанні ZTA в корпоративне середовище. Малоймовірно, що будь-яке підприємство може перейти до ZTA за один цикл оновлення технологій. Оскільки повний перехід до концепції нульової довіри є складним і тривалим процесом, у більшості організацій протягом певного часу можуть співіснувати як традиційні механізми захисту, так і елементи ZTA, що впроваджуються поступово для окремих бізнес-процесів. Успішна реалізація цього підходу вимагає забезпечення гнучкості основних компонентів, таких як керування ідентифікацією, контроль пристроїв і реєстрація подій для ефективного функціонування як у межах класичної архітектури безпеки на основі периметра, так і в гібридній архітектурі. Крім того, обрані рішення мають бути сумісними з наявною корпоративною інфраструктурою, щоб уникнути значних ускладнень під час впровадження. Варто також зазначити, що міграція до ZTA вимагатиме (як мінімум) часткової реорганізації робочих процесів в організації. Це, водночас, створює умови для впровадження сучасних методів та практик безпечної розробки систем відповідно до міжнародних стандартів [31], якщо IT-підприємства ще не зробили цього для робочих процесів.

Деякі сценарії розгортання та варіанти використання дозволяють швидко впровадити ZTA на підприємстві. Зокрема, концепція нульової довіри є ефективним підходом для організацій із розподіленою інфраструктурою або значною кількістю віддалених користувачів. Водночас будь-яке підприємство може застосовувати принципи нульової довіри для підвищення рівня безпеки, незалежно від структури чи масштабу. На практиці перехід до нової моделі безпеки зазвичай здійснюється поступово, тому в корпоративному середовищі певний час можуть співіснувати як традиційні механізми захисту на основі периметру, так і елементи ZTA.

Далі розглянемо деякі рекомендації щодо практичного впровадження ZTA, з урахуванням можливих сценаріїв, викликів і оптимальних підходів до її інтеграції в корпоративне середовище для різного роду діяльності IT-підприємств.

1.1. Підприємство з віддаленими структурними підрозділами

Найпоширенішим сценарієм є підприємство, що має центральний офіс і один або декілька географічно розподілених підрозділів (філіалів), які не з'єднані фізичною мережею, що належить підприємству (рис. 1).

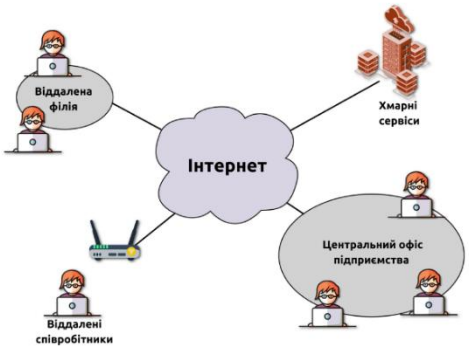

Рис. 1. Підприємство з віддаленими працівниками

При цьому працівники у віддалених підрозділах або офісах можуть не мати повноцінної локальної мережі підприємства, проте їм все одно необхідний доступ до корпоративних ресурсів для виконання своїх завдань. У таких випадках підприємство може використовувати багатопротокольну комутацію за мітками (Multiprotocol Label Switching – MPLS) для зв'язку з центральним офісом, однак пропускна здатність цього каналу може бути недостатньою для обробки всього трафіку. Крім того, підприємство може вважати недоцільним спрямовувати весь трафік, призначений для хмарних сервісів, застосунків або сервісів через центральний офіс. Аналогічна ситуація виникає, коли співробітники працюють віддалено або перебувають поза межами основної інфраструктури підприємства, використовуючи як корпоративні, так і особисті пристрої (BYOD). У таких випадках підприємство може надавати доступ до певних ресурсів, таких як електронна пошта чи корпоративний календар, водночас обмежуючи або забороняючи доступ до більш конфіденційних ресурсів (наприклад, база даних співробітників).

У цьому сценарії механізм політики (Policy Engine – PE) та адміністратор політики (Policy Administrator – PA) [7, 15] реалізується у вигляді хмарного сервісу (який зазвичай забезпечує високий рівень доступності та не вимагає від віддалених користувачів підключення до корпоративної інфраструктури для доступу до хмарних ресурсів), а кінцеві пристрої мають встановлений агент (відповідно до моделі розгортання на основі агента пристрою/шлюзу, де зазвичай у системі суб'єкта є розгорнутий користувальницький агент, що діє як точка застосування політики (Policy Enforcement Point – PEP) агента користувача) або доступ до ресурсного порталу (відповідно до моделі розгортання на основі порталу ресурсів, де PEP є єдиним компонентом, який виконує роль шлюзу для відповідних запитів). Розміщення PE/PA у локальній мережі підприємства у цьому випадку є менш ефективним, оскільки змусить віддалені філії та співробітників перенаправляти весь трафік через центральний офіс для доступу до хмарних сервісів та застосунків.

З огляду на відсутність єдиного захищеного периметра, одним із ключових викликів у такому сценарії є забезпечення безпеки корпоративних баз даних і сховищ, що можуть бути розміщені як у локальному сегменті мережі підприємства, так і у хмарному середовищі. Концепція нульової довіри вимагає, щоб кожен запит на доступ до даних, незалежно від джерела, супроводжувався ретельною і повторною перевіркою ідентичності користувача та контексту доступу. Зокрема, для ресурсів, що зберігають конфіденційну/чутливу інформацію (наприклад, персональні дані співробітників, фінансові документи чи інтелектуальну власність), впроваджується модель багаторівневого контролю доступу з динамічною адаптацією політик. Це може включати як ізоляцію критичних сховищ у сегментованих віртуальних локальних мережах (Virtual Local Area Network – VLAN), так і застосування моделей контролю

доступу на основі ролей (Role-based Access Control – RBAC) та/або атрибутів (Attribute-based Access Control – ABAC).

Крім того, у контексті доступу до конфіденційних даних дедалі актуальнішими стають механізми, що базуються на концепції «нульового знання/розголошення» (Zero-Knowledge – ZK) [32 – 36] та які можуть бути впроваджені в процеси автентифікації або перевірки дозволів, повноважень, прав. Дані механізми дозволяють довести право на доступ до ресурсу без потреби передавати або розкривати самі дані, що значно підвищує рівень конфіденційності та захищає від атак типу «людина посередині» (man-in-the-middle) або витоку даних у процесі автентифікації. Наприклад, використовуючи концепцію ZK, система може перевірити, чи має користувач необхідні повноваження для доступу до певних чутливих даних бази даних (наприклад, до даних про співробітників підприємства), не розкриваючи при цьому жодних деталей про самі повноваження або вміст ресурсу. У хмарних середовищах така технологія може бути інтегрована з постачальниками ідентифікації (Identity Provider – IdP), які здійснюють перевірку повноважень користувача без необхідності доступу до самих даних, що додатково відповідає вимогам конфіденційності та відповідності нормативним стандартам (GDPR, HIPAA тощо).

1.2. Підприємство, що функціонує у багатохмарному середовищі

Поширеним сценарієм застосування ZTA є функціонування підприємства у багатохмарному середовищі, коли використовується інфраструктура кількох хмарних провайдерів (рис. 2).

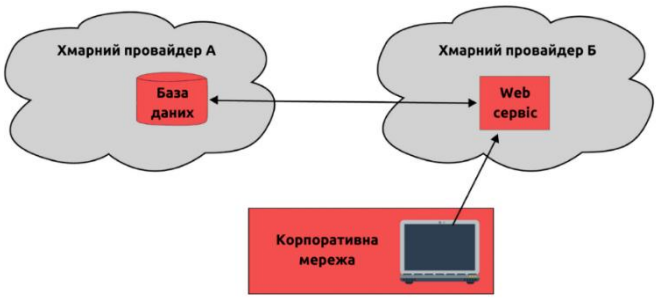

Рис. 2. Підприємство з багатохмарним середовищем

У цьому випадку підприємство має локальну мережу, проте для розміщення застосунків, сервісів і баз даних задіяні два або більше постачальників хмарних послуг. Нерідко застосунок або сервіс функціонує в одній хмарній інфраструктурі, тоді як база даних розташована в іншій. Для забезпечення ефективної роботи системи та спрощення адміністрування необхідно, щоб застосунок, розгорнутий в інфраструктурі одного хмарного провайдера *А*, мав можливість безпосередньо взаємодіяти з базою даних іншого хмарного провайдера *Б*, уникаючи маршрутизації трафіку через локальну мережу підприємства.

Цей сценарій є реалізацією серверної взаємодії (server-to-server) відповідно до специфікації програмно-визначуваного периметра (Software Defined Perimeter – SDP) від Cloud Security Alliance [37]. Проте широке застосування хмарних технологій виявило обмеження традиційної моделі безпеки, яка базується на захисті мережевого периметра та є неефективною в межах хмарного середовища. В свою чергу, ZTA передбачає, що внутрішня та зовнішня інфраструктури мають однаковий рівень довіри, тобто фізичне розташування ресурсів не повинно впливати на рівень безпеки доступу (не повинно бути ніякої різниці між мережевою інфраструктурою, що належить і експлуатується підприємством, і інфраструктурою, що належить і експлуатується будь-яким іншим постачальником послуг). Тому, для забезпечення контролю доступу в багатохмарному середовищі PEP розміщуються на рівні застосунків, сервісів і баз даних. В свою чергу PE/PA можуть бути інтегровані як у межах одного із задіяних хмарних провайдерів, так і в незалежному середовищі третьої сторони. Користувачі отримують доступ до ресурсів через портал або встановлений агент, звертаючись до відпові-

дних PEP. Такий підхід дає змогу підприємству контролювати доступ до своїх ресурсів незалежно від місця їх розташування.

Варто зазначити, що у процесі проєктування та розгортання ZTA в багатохмарному середовищі важливим аспектом є забезпечення безпеки баз та сховищ даних, які використовуються на різних етапах обробки, передачі та зберігання інформації. У контексті моделі, наведеної на рис. 2, особливу увагу слід приділити захисту баз та сховищ даних, що знаходяться під контролем хмарного провайдера *А*, але обслуговують застосунки, розгорнуті в інфраструктурі хмарного провайдера *Б*. Такий формат взаємодії між хмарними провайдерами створює додаткові вектори загроз, які не можуть бути належним чином враховані у межах традиційної моделі безпеки. У зв'язку з цим обов'язковою умовою є впровадження механізмів доступу до баз і сховищ даних, які базуються на принципах мінімальних привілеїв, автентифікації та авторизації на основі контексту, а також на криптографічних механізмах, що підтримують концепцію ZK. Такі механізми дозволяють підтвердити права доступу без безпосереднього розкриття ідентифікаційних даних, що суттєво знижує ризики компрометації у випадку перехоплення або несанкціонованого втручання в канали зв'язку (це дозволяє істотно підвищити стійкість системи до атак типу «людина посередині», атак повторного відтворення (replay attacks), а також до витоку ідентифікаційних даних у результаті компрометації одного з провайдерів). Сьогодні існує різні підходи доказів із нульовим розголошенням (Zero-knowledge proofs – ZKP), зокрема, інтерактивні та неінтерактивні [38]. Для хмарного середовища більш релевантними є неінтерактивні ZKP, які не вимагають багатоетапної взаємодії між сторонами, що знижує затримки при обробці запитів і дозволяє реалізовувати масштабовані рішення для контролю та керування доступу до розподілених ресурсів. Одним із відомих прикладів таких протоколів є *zk-SNARK* [39], які використовуються в низці проєктів, орієнтованих на конфіденційність. Єдине, що в даному випадку є важливим, це те, що їхнє впровадження в архітектуру доступу до хмарних сховищ забезпечує можливість підтвердження автентичності без необхідності передачі паролів, токенів або інших сенситивних атрибутів. Крім того, всі бази та сховища даних, незалежно від їх фізичного або хмарного розміщення, повинні розглядатися як середовища з невизначеним рівнем довіри. Це передбачає, що всі дані мають зберігатися та передаватися виключно у зашифрованому вигляді, з використанням сучасних алгоритмів симетричного та асиметричного шифрування, протоколів TLS 1.3 або/та QUIC для захисту даних на транспортному рівні, а також з обов'язковим застосуванням наскрізного шифрування для захисту даних в стані спокою, під час обробки та під час передавання. Додатково, необхідно впровадити регулярний аудит політик доступу, що забезпечить своєчасне виявлення аномалій та спроб несанкціонованого доступу. Інтеграція таких засобів із PEP, які контролюють кожен запит до ресурсу, дозволяє забезпечити дотримання принципів концепції нульової довіри незалежно від середовища розгортання (навіть у середовищі, де кілька хмарних провайдерів відповідають за різні компоненти інфраструктури підприємства). У сукупності ці підходи дозволяють створити стійку до компрометації архітектуру, здатну гарантувати безпечну взаємодію між компонентами підприємства навіть у розподіленому хмарному ландшафті з неоднорідними вимогами до безпеки з боку різних постачальників послуг.

Таким чином, у даному сценарії критичним є забезпечення повноцінного контролю над кожним етапом доступу до ресурсів підприємства, від початкового підключення до мережі – до виконання конкретного запиту до внутрішніх ресурсів. Реалізація принципів нульової довіри у такому середовищі вимагає застосування комплексної моделі захисту, яка поєднує мікросегментацію інфраструктури, динамічну автентифікацію на основі контекстних факторів, надійні криптографічні механізми, включаючи ZK, а також постійний моніторинг активності користувачів. Впровадження таких механізмів у межах політики найменших привілеїв, а також RBAC та/або ABAC, забезпечує не лише захист конфіденційної інформації, але й унеможливлює бічне переміщення всередині мережі та несанкціоноване підвищення привілеїв. Як результат, навіть за умови різного ступеня довіри до користувачів і систем та у

межах розподіленої структури доступу, підприємство зберігає контроль над своїми внутрішніми ресурсами, знижуючи ризики як зовнішніх, так і внутрішніх загроз.

1.3. Підприємство з контрактними послугами та/або доступом для позаштатних користувачів

Одним із поширених сценаріїв є підприємство, яке надає обмежений доступ до своїх ресурсів відвідувачам та/або стороннім постачальникам послуг, що виконують контрактні зобов'язання (рис. 3).

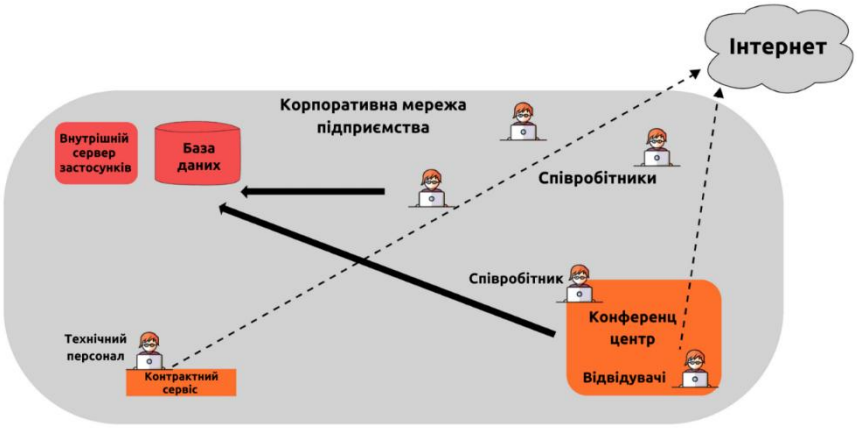

Рис. 3. Підприємство з доступом для позаштатних працівників

Таке підприємство має власні внутрішні застосунки, сервіси, бази даних та інші активи. Деякі з них можуть обслуговуватися за контрактом залученими постачальниками, які можуть періодично відвідувати підприємство для забезпечення технічного обслуговування, наприклад, системи керування розумного опалення або освітлення, що знаходяться у власності та під управлінням зовнішніх компаній. Для виконання своїх завдань такі постачальники та відвідувачі потребують підключення до мережі. У межах ZTA підприємство може організувати даний процес таким чином, щоб забезпечити доступ технічному персоналу, який відвідує підприємство, або його пристроям до мережі Інтернет, водночас унеможливлюючи несанкціонований доступ до своїх внутрішніх ресурсів.

Крім того, підприємство може мати конференц-центр, де відвідувачі взаємодіють зі співробітниками. У рамках ZTA, реалізованої за допомогою концепції SDP, пристрої та суб'єкти автентифікації розмежовуються, що дозволяє співробітникам отримувати доступ до необхідних корпоративних ресурсів, тоді як відвідувачі можуть користуватися лише доступом до мережі Інтернет. Більше того, вони не мають змоги виявити внутрішні сервери або сервіси підприємства за допомогою мережевого сканування, що запобігає активній розвідці мережі та бічному переміщенню. У цьому сценарії PE/PA можуть бути реалізовані як хмарний сервіс або розміщені локально (за умови, що хмарні сервіси майже не використовуються на підприємстві або використовуються тільки для окремих сервісів). Доступ до корпоративних ресурсів може здійснюватися через встановлений агент на кінцевих пристроях користувачів (відповідно до моделі розгортання на основі агента пристрою/шлюзу, де зазвичай у системі суб'єкта є розгорнутий користувальницький агент, що діє як PEP агента користувача) або через портал (відповідно до моделі розгортання на основі порталу ресурсів, де PEP є єдиним компонентом, який виконує роль шлюзу для відповідних запитів). При цьому механізм PA гарантує, що всі некорпоративні активи (тобто пристрої, які не мають встановленого агента або не можуть під'єднатися до порталу) не матимуть доступу до локальних ресурсів, а лише до мережі Інтернет.

Окрім зазначеного вище, в умовах реалізації ZTA в даному сценарії, ключове значення має безпека корпоративних баз і сховищ даних, що інтегровані у внутрішню мережу підприємства та взаємодіють із внутрішніми сервісами і авторизованими суб'єктами доступу. Відповідно до принципів нульової довіри доступ до таких ресурсів повинен здійснюватися

виключно після автентифікації суб'єкта та динамічної авторизації кожного окремого запиту із залученням механізмів оцінки контексту доступу, що враховує не лише ідентифікаційні атрибути суб'єкта, а й технічні характеристики пристрою, зокрема тип пристрою, часові параметри запиту, місцезнаходження, попередню поведінку при доступі, рівень ризику, поведінкові атрибути та інші параметри, які визначаються динамічною політикою контролю доступу для забезпечення глибокого аналізу подій у випадку прийняття рішення про надання доступу або при виникненні інцидентів безпеки.

В свою чергу, внутрішні сховища даних повинні бути ізольованими від загальної корпоративної мережі на рівні маршрутизації та міжмережевих політик, із застосуванням принципу мікросегментації. Усі запити до таких ресурсів повинні проходити виключно через PEP, які, у взаємодії з точкою прийняття рішення про політику (Policy Decision Point – PDP) та відповідно до принципу найменших привілеїв, забезпечують надання доступу лише до тієї інформації, яка є необхідною для виконання конкретного службового завдання, без можливості несанкціонованого доступу до інших частин системи, переміщення між сегментами мережі або підвищення привілеїв (privilege escalation). Водночас, навіть за умов впровадження мікросегментації мережевої інфраструктури та ізоляції внутрішніх сховищ даних, постає потреба у застосуванні додаткових механізмів безпеки, орієнтованих безпосередньо на забезпечення конфіденційності та цілісності інформації, яка зберігається. У цьому контексті ключову роль відіграють сучасні криптографічні механізми, зокрема методи шифрування та протоколи підтвердження прав доступу на основі концепції ZK, які дозволяють підтверджувати достовірність даних або ідентичність суб'єкта без передачі самих даних стороні, що здійснює перевірку та прийняття рішення. Це значно знижує ризики витоку конфіденційної інформації, зокрема у випадках, коли певні компоненти інфраструктури виявляються вразливими або скомпрометованими. Застосування зазначених механізмів має бути інтегрованим у загальну модель контролю доступу, що реалізується в межах ZTA, із дотриманням принципу найменших привілеїв, а також із використанням моделей контролю доступу RBAC та/або ABAC. Це забезпечує гнучке та динамічне керування доступом із урахуванням поточного контексту запиту та рівня довіри до суб'єкта, що мінімізує ризики бічного переміщення або підвищення привілеїв. Крім того, усі запити на отримання доступу до баз і сховищ даних повинні фіксуватися у спеціалізованих журналах подій із забезпеченням цілісності відповідних записів, їх подальшою перевіркою та автоматизованим аналізом у рамках постійного моніторингу. Даний підхід дозволяє своєчасно виявляти спроби порушення політик доступу, ознаки аномальної поведінки або інші події, що можуть свідчити про потенційну загрозу.

Таким чином, у контексті сценарію з підвищеним рівнем ризику, зокрема за участі зовнішніх підрядників, ефективне керування доступом до внутрішніх сховищ даних вимагає впровадження багаторівневої моделі безпеки. Така модель має ґрунтуватися на мікросегментації інфраструктури, динамічній авторизації, застосуванні криптографічних механізмів захисту, включно з ZK та безперервному моніторингу. Комплексне поєднання цих підходів забезпечує реалізацію принципів нульової довіри та сприяє формуванню адаптивного й стійкого механізму захисту корпоративних інформаційних ресурсів.

1.4. Співпраця між підприємствами

Співпраця між підприємствами є ще одним поширеним сценарієм (наприклад, реалізація спільного проєкту може передбачати залучення співробітників двох підприємств (рис. 4)). Ці підприємства можуть бути окремими державними установами або навіть державною установою та приватним підприємством. У цьому випадку, відповідно до рис. 4, *Підприємство А* керує базою даних, необхідною для виконання проєкту, і повинне надати доступ до певної інформації окремим співробітникам *Підприємства Б*. Найпростішим підходом може бути створення спеціальних облікових записів для співробітників *Підприємства Б* з доступом лише до необхідних даних, проте такий підхід ускладнює керування доступом у міру зростання кількості користувачів. Використання централізованої системи керування ідентифіка-

цією дозволяє спростити цей процес, за умови, що PEP обох підприємств підтримують автентифікацію суб'єктів у межах спільної системи керування ідентифікацією.

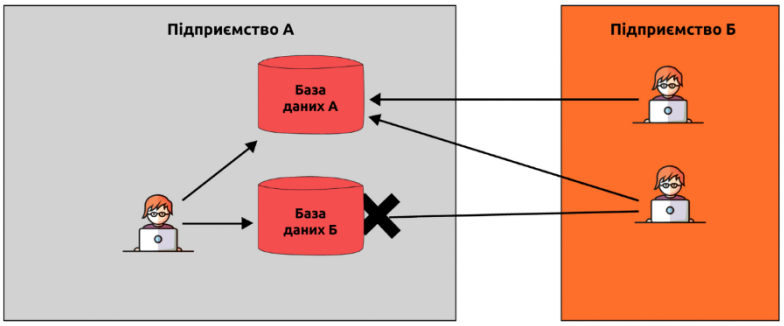

Рис. 4. Сценарій взаємодії між підприємствами

Даний сценарій частково подібний до сценарію підприємства з віддаленими структурними підрозділами, оскільки співробітники обох підприємств можуть працювати поза межами корпоративної мережі, а необхідний для них ресурс може бути розміщений як у локальному середовищі підприємства, так і в хмарному середовищі. Це усуває необхідність налаштовувати складні правила для міжмережевих екранів або створювати розширені списки контролю доступу (Access Control List – ACL), що визначають певні IP-адреси *Підприємства Б,* які можуть отримати доступ до ресурсів *Підприємства А* на основі політик доступу *Підприємства А*. Так само, як і у сценарії підприємства з віддаленими структурними підрозділами, використання PE/PA, які розгорнуті у хмарному середовищі, може забезпечити доступність ресурсів для співробітників обох підприємств без необхідності створення віртуальної приватної мережі (Virtual Private Network – VPN) або подібних рішень. Співробітники *Підприємства Б* можуть отримати доступ до необхідних ресурсів шляхом встановлення клієнтського ПЗ (наприклад, агента на кінцевому пристрої) або через відповідний безпечний/захищений веб-шлюз (Secure Web Gateway – SWG), відповідно до моделі розгортання на основі порталу ресурсів, де PEP є єдиним компонентом, який виконує роль шлюзу для відповідних запитів.

Однак у випадку співпраці між підприємствами захист баз і сховищ даних вимагає впровадження додаткових механізмів, які враховують використання корпоративних ресурсів зовнішніми користувачами. Навіть за умови обмеження доступу до частини інформації, залишається ризик порушення цілісності або розголошення даних унаслідок помилок у налаштуванні прав доступу або зламу засобів захисту. Для мінімізації таких ризиків, бази даних мають проєктуватися відповідно до принципу найменших привілеїв, що передбачає розмежування даних за типом інформації, ролями та/або атрибутами користувачів. На практиці це, наприклад, може досягатися шляхом використання віртуальних таблиць (уявлень – view) у системах керування традиційними базами даних, або впровадження політик обмеження доступу до окремих полів у нереляційних сховищах. Зовнішнім користувачам надається доступ лише до певних уявлень, причому сам доступ здійснюється через відповідні шлюзи PEP, які перевіряють не тільки облікові дані користувача, але й додаткові атрибути, серед яких можуть бути, наприклад, роль, тип пристрою, часові параметри запиту, місцезнаходження, попередня поведінка при доступі, тип та стан сеансу, поведінкові атрибути тощо. Це дозволяє застосовувати динамічні правила доступу, які враховують поточні умови взаємодії.

Проте захист даних вимагає також збереження конфіденційності не лише їхнього змісту, але й фактів звернення до них. У випадках обробки фінансової, службової або технічної інформації навіть доступ до метаданих може становити загрозу витоку. Для усунення подібних ризиків у рамках ZTA повинні застосовуватися механізми, що забезпечують безпеку даних на основі концепції ZK, тобто механізмів, які забезпечують підтвердження прав доступу без передачі облікових даних або їх атрибутів. Зокрема, використання протоколів на основі *zk-SNARK* або *zk-STARK* [40] у межах хмарних шлюзів дозволяє перевіряти рівень доступу користувача без розкриття його ідентифікатора чи змісту даних, до яких здійснюється запит.

Інтеграція механізмів ZK в ZTA забезпечує керований доступ до інформації незалежно від місцезнаходження користувача або типу пристрою. Всі перевірки здійснюються на рівні PEP, що поєднують політики безпеки організації із атрибутами (характеристиками) користувача та середовища доступу. Завдяки цьому ресурси залишаються ізольованими, а доступ надається лише за умов, які є достатніми й обґрунтованими з позиції безпеки. Однак постійний розвиток IT-технологій потребує ще глибшої інтеграції таких підходів безпосередньо у внутрішню архітектуру інформаційних систем, зокрема, інтеграції механізмів ZK безпосередньо у системи керування базами даних. Щодо цього, цікавий підхід до використання концепції ZK для баз даних запропонований у роботі [41]. Такі рішення відкривають нові можливості для побудови середовищ із підвищеним рівнем довіри навіть в інфраструктурі із спільним використанням ресурсів або під час обробки даних у спільних інформаційних системах.

1.5. Підприємство, що надає публічні або сервісні послуги

Підприємства, що надають публічні або сервісні послуги, можуть працювати з користувачами, які не є частиною організації, але взаємодіють із її цифровими ресурсами. Доступ до таких ресурсів може вимагати або не вимагати реєстрації користувачів, тобто створення ними облікових записів або отримання наданих підприємством облікових даних. Такі сервіси можуть бути розраховані на широке коло користувачів (наприклад, загальнодоступні інформаційні портали) або обмежену групу (наприклад, клієнтів компанії чи певних зовнішніх суб'єктів). У всіх цих випадках є ймовірність, що доступ до ресурсів здійснюється з пристроїв, які не належать підприємству, а отже, можливості застосування корпоративних політик кібербезпеки є обмеженими.

Якщо доступ до ресурсу здійснюється без реєстрації (наприклад, загальнодоступний веб-сайт або веб-сервіс), застосування принципів ZTA є обмеженим, оскільки підприємство не може контролювати стан пристроїв, із яких надходять запити, або встановлювати власні політики доступу. В разі, якщо користувачі проходять процедуру реєстрації, підприємство може запроваджувати власні політики безпеки, серед яких вимоги до складності паролів, їхнього життєвого циклу та інших параметрів, а також використання MFA. Водночас можливості впровадження більш детальних політик залишаються обмеженими для цієї категорії користувачів, оскільки підприємство не контролює їх зовнішні пристрої. В такому разі, аналіз вхідних запитів може відігравати важливу роль у моніторингу стану сервісу та виявленні потенційних кібератак, що імітують дії легітимних користувачів. Наприклад, якщо зареєстровані користувачі зазвичай отримують доступ до порталу за допомогою певного набору типових веб-браузерів, а система фіксує аномальне зростання запитів із невідомих типів браузерів або відомих застарілих версій, що може свідчити про автоматизовану атаку. У такому випадку підприємство може вжити заходи для обмеження запитів від виявлених клієнтів або впровадити додаткові механізми перевірки для подібних запитів. Крім того, підприємство повинне враховувати чинні законодавчі норми та вимоги щодо збору, обробки та зберігання даних користувачів, які взаємодіють із сервісом.

Окрему увагу в цьому сценарії необхідно приділити безпеці баз і сховищ даних, що використовуються для зберігання облікових записів, журналів доступу, історії транзакцій та інших персональних і конфіденційних даних користувачів. Використання концепції нульової довіри передбачає обмеження доступу до таких ресурсів навіть серед внутрішніх суб'єктів підприємства, тобто кожен запит до бази даних повинен здійснюватися лише суб'єктами, які пройшли автентифікацію та відповідати визначеним політикам безпеки. Наприклад, замість надання безперервного доступу для сервісу до бази даних користувачів, можна впровадити тимчасові облікові токени автентифікації з обмеженим терміном дії та визначеними правами доступу, що зменшує ризики у разі компрометації окремої компоненти системи. Крім того, підвищення рівня захисту може бути досягнуто завдяки впровадженню механізмів ZK, які дозволяють системі з нульовою довірою переконатися, що суб'єкт є справжнім (автентичним), а запит дійсним. PDP/PEP приймає належне рішення, щоб дозволити суб'єкту отрима-

ти доступ до ресурсу. Це знижує ризик витоку критичної інформації у разі перехоплення мережевого трафіку або успішної атаки на один із проміжних вузлів інфраструктури. В свою чергу керування доступом залежить від стану безпеки пристрою (механізму, засобу) та інших ситуативних факторів (наприклад, часу та місцезнаходження, попередньої поведінки при доступі тощо), які можуть вплинути на рівень довіри до того, як доступ до ресурсу буде наданий відповідно до певних політик. Загалом, підприємствам необхідно розробити та підтримувати динамічну політику доступу до ресурсів, що базується на оцінці ризиків, і налаштувати систему, яка гарантуватиме правильне та послідовне застосування цих політик для окремих запитів на доступ. Підприємству не слід покладатися на передбачувану надійність, коли суб'єкт відповідає базовому рівню автентифікації (наприклад, при вході до системи), а усі наступні запити до ресурсів вважаються однаково дійсними. Проте важливо розуміти, що при впровадженні таких підходів необхідно забезпечити баланс між рівнем безпеки та зручністю для користувачів, що особливо критично для ресурсів, орієнтованих на широку аудиторію.

В цілому реалізація ZTA є досить складним процесом, причому це швидше за все шлях (рух), ніж повна заміна інфраструктури або технологічних процесів. Тому підприємство повинне прагнути до поступового впровадження принципів нульової довіри, змін у процесах та технологічних рішень, які захищають її найцінніші активи даних. Більшість підприємств, швидше за все, продовжуватимуть працювати у комбінованому режимі з використанням нульової довіри та периметра протягом невизначеного періоду часу, продовжуючи вкладати кошти у постійну модернізацію IT [7]. При цьому наявність плану модернізації IT, що включає перехід до ZTA, може допомогти підприємству сформувати дорожні карти для здійснення невеликих (поступових) переходів на нові робочі процеси. Зрештою, те, як підприємство переходитиме на концепцію нульової довіри, буде залежати від його поточного стану кібербезпеки та операційної діяльності. Причому підприємство має досягти базового рівня підготовленості (базовий рівень включає визначення та класифікацію активів, суб'єктів, бізнес-процесів, потоків даних і відображення залежностей для підприємства), перш ніж стане можливим розгорнути масштабну систему, орієнтовану на нульову довіру. Підприємству необхідна ця інформація, щоб визначити список бізнес-процесів-кандидатів та суб'єктів/активів, які будуть залучені до цього процесу. При цьому, найбільшою проблемою, що перешкоджає впровадженню успішних рішень в області нульової довіри, на думку фахівців ACT-IAC (American Council for Technology and Industry Advisory Council – Американська рада з технологій та Консультативна рада з питань промисловості), може бути загальний недостатній рівень кібербезпеки [42]. Ними зазначається, наприклад, що більшість державних установ не мають фундаментальних основ (таких як, політик, процесів та інструментів), необхідних для розгортання систем, що відповідають концепції нульової довіри.

Таким чином, можна зробити висновок, що процес впровадження ZTA повинен бути поступовим та орієнтованим на розвиток існуючих технологій та IT-середовищ в організації. Для цього необхідно розробляти і тестувати різні практичні рішення ZTA, керуючись загальноприйнятими принципами та рекомендаціями в галузі кібербезпеки. Важливим аспектом є детальний аналіз архітектури кожного рішення, використаних технологій, специфічних конфігурацій та інтеграцій, а також їх відповідності сучасним стандартам кібербезпеки та регуляторним вимогам. Тому, кожна організація повинна розробляти власну стратегію впровадження ZTA, оскільки єдиного універсального підходу не існує. ZTA є не технічним стандартом, а концептуальною моделлю, що передбачає постійне вдосконалення політик і процесів керування доступом відповідно до її принципів. При цьому доречно відразу ж звернути увагу на те, що керівництво IT-підприємства має прагнути до поступового впровадження принципів нульової довіри, зміни процесів та технологічних рішень, що захищають його найцінніші активи даних. Такий поступовий підхід дозволить знизити ризик відмов і помилок у системі, допоможе зрозуміти подальші процеси розгортання елементів системи, а також полегшить перехід персоналу до нової архітектури.

2. Пропонована модель впровадження архітектури нульової довіри

Залежно від того як налаштовано корпоративну мережу для різних бізнес-процесів на одному підприємстві можуть використовуватися кілька моделей розгортання ZTA. У цьому контексті для розуміння доцільно звернутися до розробленої відповідно до загальноприйнятих галузевих та академічних принципів нульової довіри Міністерством оборони США так званої моделі стовпів та можливостей [43, 44] (див. рис. 5).

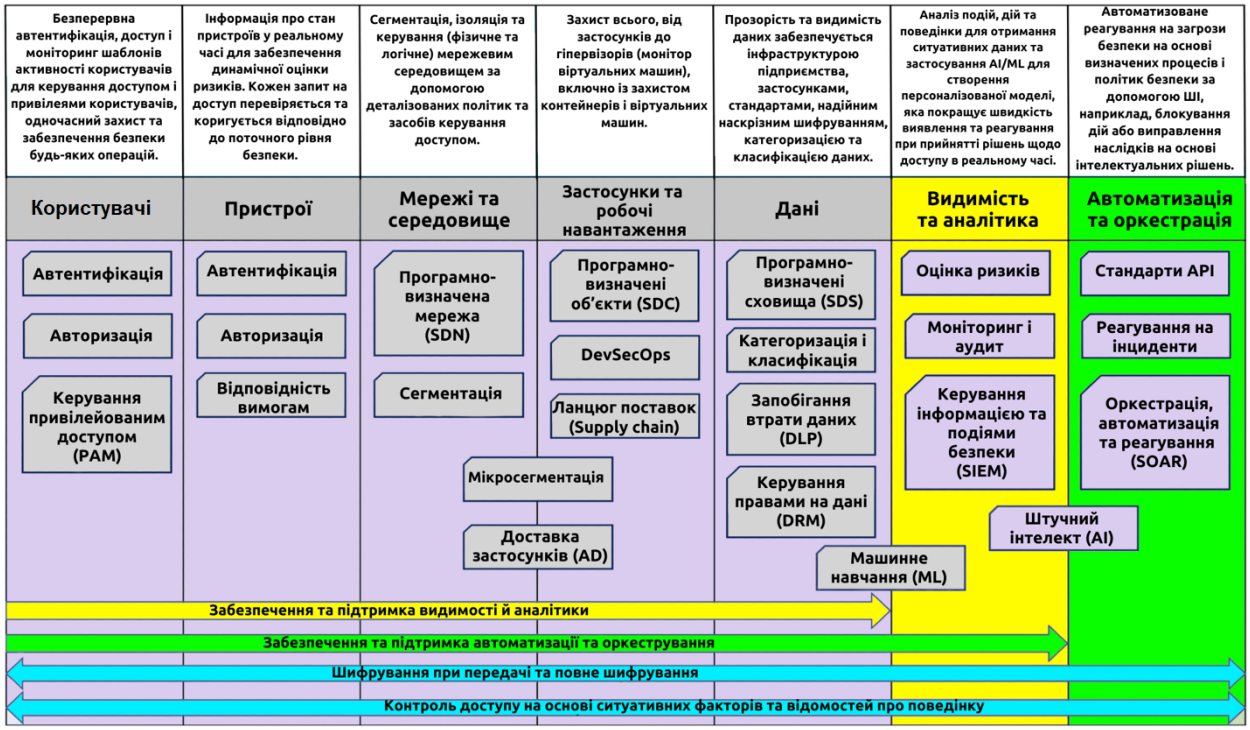

Рис. 5. Стовпи та можливості моделі впровадження архітектури нульової довіри

Стовп (*pillar*) – це ключова область для впровадження систем контролю/захисту нульової довіри У моделі, що розглядається, їх сім: користувачі, пристрої, мережі та середовища, застосунки та робочі навантаження, дані, видимість та аналітика, а також автоматизація та оркестрація. *Можливості* (*capabilities*) – це здатність досягати бажаного ефекту відповідно до певних стандартів та умов за допомогою комбінації способів і засобів (дій та ресурсів) для виконання певного набору дій. Стовпи асоціюються з такими можливостями, як автентифікація ідентифікаційних даних (особистості) та програмно-визначуване підприємство (Software Defined Enterprise). Загалом, запропонована вище модель передбачає використання різних механізмів (способів, засобів) автентифікації та авторизації користувачів і пристроїв, керування привілейованим доступом (Privileged Access Management – PAM), мікросегментацію мережі, програмно-визначену інфраструктуру (SDN, SDC, SDS), контроль доступу до даних (DRM, DLP), підхід DevSecOps (Development, Security, and Operations), а також рішення для моніторингу, оцінки ризиків і реагування на інциденти (SIEM, SOAR, AI/ML) тощо. Усі ці елементи працюють у взаємозв'язку, забезпечуючи видимість і аналітику, автоматизацію та оркестрацію процесів безпеки, шифрування при передачі та повне шифрування, а також ефективний контроль доступу на основі ситуативних факторів та відомостей про поведінку. Для досягнення належної інтеграції між стовпами та можливостями потрібно всеосяжне управління. Основні стовпи та можливості забезпечують максимальну видимість та захист даних, що є ключовим моментом за будь-якої реалізації нульової довіри. У цьому сенсі, стовпи моделі нульової довіри можна представити у вигляді взаємопов'язаних частин пазла навколо стовпа даних, оточеного стовпами захисту [44]. Усі стовпи захисту працюють у комплексі для ефективного захисту стовпа даних. Взаємодія цих компонентів забезпечує функціонування корпоративного середовища відповідно до принципів ZTA.

Аналіз представленої на рис. 5 моделі дозволяє зробити висновок, що для її впровадження необхідно використовувати кілька моделей розгортання ZTA (див. п. 1), зокрема, моделі розгортання з мікросегментацією, з використанням хмарної маршрутизації, на основі ресурсів. Тобто цю модель певною мірою через охоплення різних моделей розгортання можна вважати комплексною, яка потребує узгодженого застосування технологій та механізмів безпеки для забезпечення належного рівня захисту корпоративного середовища. У зв'язку з цим постає питання стандартизації впровадження принципів нульової довіри. Попри відсутність єдиної загальноприйнятої методології, все ж таки деякий підхід впровадження було запропоновано Міністерством оборони США [45]. У цьому підході/моделі застосовуються/передбачаються два списки стандартів, а саме так звані профільні стандарти (Standards Profile – StdV-1) і стандарти прогнозування (Standards Forecast – StdV-2), що забезпечує системний підхід до впровадження ZTA в інформаційних системах. Профільні стандарти визначають набір технологій, нормативно-правових актів, політик, а також тактик, технік і процедур, що регулюють функціонування компонентів нульової довіри. Стандарти прогнозування охоплюють технологічні, операційні та бізнес-стандарти, що визначають перспективні напрями розвитку можливостей нульової довіри, а також майбутні вимоги до їхньої реалізації. Це забезпечує структурований підхід до впровадження ZTA, поєднуючи як поточні регуляторні вимоги, так і стратегічне планування розвитку архітектури. У табл. 2 представлено набори можливостей, запропоновані Міністерством оборони США [44], що відповідають різним рівням забезпечення безпеки та захисту *даних, застосунків, активів* та *послуг* (*data, applications, assets and services* – DAAS) для кожного стовпа нульової довіри, пов'язані з поетапністю впровадження ZTA на підприємстві.

Цільовий рівень (*Target Level*) – це мінімальний набір можливостей нульової довіри та видів діяльності (activities), необхідних для забезпечення безпеки та захисту даних, застосунків, активів та послуг. Кожна можливість нульової довіри відповідає одному із семи стовпів нульової довіри. Незважаючи на те, що повний набір можливостей охоплює діапазон від цільового (*Target*) до просунутого/розширеного рівня (*Advanced*), деякі можливості досягаються лише на цільовому рівні, а деякі лише на розширеному. Більшість можливостей мають асоційовані активності (види діяльності) як на цільовому рівні, так і на просунутому/розширеному рівні нульової довіри. Подібний підхід дозволяє поступово впроваджувати необхідні заходи безпеки, починаючи з критично важливих механізмів та завершуючи їхньою повною інтеграцією у всі аспекти керування кіберзахистом підприємства. *Цільовий* (*Target*) або *базовий рівень* охоплює критично необхідні механізми захисту та передбачає впровадження інвентаризації користувачів і пристроїв, уніфіковане керування кінцевими пристроями, визначення потоків даних та застосування принципу найменших привілеїв тощо. Дані механізми є основою для подальшого розвитку архітектури безпеки. В свою чергу *середній* (*Target & Advanced*) *рівень* розширює функціональність шляхом впровадження додаткових механізмів ідентифікації, MFA, контролю відповідності пристроїв вимогам безпеки, програмно-визначених мереж, мікросегментації тощо. Також реалізуються механізми авторизації пристроїв у режимі реального часу, контроль їх відповідності політикам безпеки та розширений моніторинг активності користувачів, що дозволяє оперативно реагувати на потенційні загрози. *Розширений* (*Advanced*) *рівень* включає динамічні методи контролю доступу, такі як безперервна автентифікація та аналіз поведінкових факторів. Здійснюється автоматизація процесів кібербезпеки, впровадження інтелектуальних механізмів реагування та запобігання втраті даних. Додатково впроваджуються ШІ та автоматизація політик безпеки, що підвищує рівень адаптивності системи безпеки. Водночас, варто зазначити, що окрім вище вказаного визначаються інструменти реалізації, що охоплюють як технічні, так і організаційні аспекти при впровадженні ZTA, зокрема стратегічне планування, матеріальне забезпечення, навчання персоналу та розробку політик безпеки. Тому, враховуючи поступовий характер впровадження, більшість функціональних можливостей реалізується поетапно,

охоплюючи як базовий, так і середній рівні, що забезпечує ефективне впровадження та адаптацію організації до принципів нульової довіри.

Таблиця 2

Набори можливостей моделі впровадження архітектури нульової довіри

	Цільовий рівень, що відповідає певному набору можливостей нульової довіри, необхідних для забезпечення безпеки та захисту DAAS		
	Target (мінімальний набір)	***Target & Advanced*** (мінімальний і розширений набір)	***Advanced*** (розширений набір)
Користувачі	✓ Інвентаризація користувачів. ✓ Принцип найменших привілеїв.	✓ Керування привілейованим доступом (PAM) та контрольований доступ користувачів. ✓ Багатофакторна автентифікація. ✓ Механізм Identity Federation. ✓ Контроль доступу на основі ситуативних факторів, відомостей про поведінку, біометрії. ✓ Безперервна автентифікація. ✓ Впровадження платформи ICAM.	
Пристрої	✓ Частково та повністю автоматизоване керування активами, вразливостями та виправленнями. ✓ Уніфіковане керування кінцевими та мобільними пристроями.	✓ Авторизація пристроїв з перевіркою в режимі реального часу. ✓ Контроль пристроїв та відповідність вимогам. ✓ Інвентаризація пристроїв та віддалений доступ. ✓ Захист кінцевих точок і розширене виявлення та реагування (EDR і XDR).	
Мережі та середовище	✓ Визначення потоків даних. ✓ Макросегментація.	✓ Програмно-визначені мережі. ✓ Мікросегментація.	
Застосунки та робочі навантаження	✓ Інвентаризація застосунків. ✓ Керування ризиками програмного забезпечення.	✓ Безпечна розробка та впровадження програмного забезпечення. ✓ Авторизація та інтеграція ресурсів.	✓ Безперервний моніторинг та постійні авторизації.
Дані	✓ Керування ризиками баз, сховищ даних. ✓ Керування корпоративними даними.	✓ Категоризація і класифікація даних. ✓ Моніторинг та аналіз даних, керування доступом до даних. ✓ Шифрування даних та керування правами. ✓ Запобігання втрати даних (DLP).	
Видимість та аналітика	✓ Ведення журналу всього трафіку та впровадження розвідки загроз. ✓ Загальна аналітика безпеки та ризиків.	✓ Керування інформацією та подіями безпеки (SIEM). ✓ Аналіз поведінки користувачів і суб'єктів (UEBA).	✓ Автоматизовані динамічні політики.
Автоматизація та оркестрація	✓ Машинне навчання. ✓ Стандартизація API.	✓ Точка прийняття рішень (PDP) та оркестрування політик. ✓ Автоматизація процесів. ✓ Оркестрація, автоматизація та реагування (SOAR). ✓ Операційний центр безпеки (SOC) і реагування на інциденти (IR).	✓ Штучний інтелект.

Спираючись на досвід впровадження систем нульової довіри відомими у світі різними організаціями та компаніями, у роботі [15] були сформульовані деякі рекомендації щодо успішного впровадження ZTA на типовому IT-підприємстві у вигляді послідовності деяких кроків/етапів. Орієнтуючись на роботу [15], а також на перевірені практики та дослідження викладені вище, можна розробити більш ефективну модель для впровадження ZTA, яка в тому числі використовуватиме і можливості вже існуючої інфраструктури інформаційної

системи підприємства. Пропонований далі підхід дозволить ретельно та продумано застосовувати засоби контролю ZTA, які найкраще захищають бізнес, водночас не створюючи перешкод для його основних операційних процесів та гнучкої роботи в умовах сучасного цифрового середовища.

Як відомо, перш ніж розпочати впровадження ZTA на підприємстві, необхідно провести детальний аналіз активів, суб'єктів, потоків даних та робочих процесів. Це дозволить отримати повне уявлення про поточний стан операційної діяльності та визначити необхідні зміни в інфраструктурі. Крім того, щоб IT-підприємство, побудоване на основі принципів нульової довіри, могло успішно функціонувати, PE повинен мати знання про суб'єктів підприємства, серед яких можуть бути як фізичні користувачі, так і нефізичні сутності, зокрема облікові записи сервісів, що взаємодіють із ресурсами [15]. Водночас, концепція нульової довіри може бути ефективно інтегрована з підходом розробки ПЗ та IT-операцій (Development and Operations – DevOps), який сприяє автоматизації процесів життєвого циклу ПЗ, включно з його розробкою, тестуванням, інтеграцією та розгортанням. DevOps забезпечує швидку адаптацію інформаційних систем до змін, підвищуючи їхню ефективність та стійкість [19, 46, 47]. Додатково, інтеграція механізмів безпеки на всіх етапах життєвого циклу можлива завдяки розширеному підходу DevSecOps, який орієнтований на проактивне виявлення загроз та мінімізацію вразливостей ще до розгортання рішень [48, 49]. Інтеграція DevSecOps у процес впровадження ZTA дозволяє створити циклічний процес управління безпекою, що включає безперервний моніторинг, ефективне реагування на кіберзагрози, аналіз ризиків, адаптивне оновлення політик доступу. Такий підхід підвищує ефективність міграції до ZTA, знижує ймовірність збоїв під час переходу та забезпечує узгодженість роботи інформаційних систем із сучасними вимогами кібербезпеки. Крім того, цей підхід дозволяє підприємству підвищити якість і стабільність роботи сервісів, а також скоротити час розгортання продуктів завдяки швидкому отриманню зворотного зв'язку від користувачів. З точки зору впровадження ZTA, підхід DevSecOps дозволяє оптимізувати процес міграції, оскільки обидва підходи базуються на поступових ітераціях, високій залученості зацікавлених сторін та постійному моніторингу результатів. Таким чином, використання DevSecOps у поєднанні з ZTA дозволяє не лише покращити керованість процесом міграції, а й мінімізувати будь-які ризики, пов'язані з його впровадженням.

Впровадження ZTA потребує структурованого підходу, що враховує як технічні, так і організаційні аспекти. Враховуючи виклики та вимоги щодо впровадження ZTA, пропонується модель впровадження, яка включатиме кілька ключових процесів. Назвемо їх: 1) стратегія нульової довіри, 2) оцінка середовища підприємства, 3) підготовка до впровадження ZTA, 4) перехід до ZTA, 5) моніторинг, обслуговування та оптимізація ZTA.

Оскільки підхід DevSecOps орієнтований на автоматизацію, ітеративний підхід і постійний контроль безпеки, запропонована модель передбачає інтеграцію даних принципів на всіх етапах впровадження ZTA. Це дозволяє не лише підвищити стійкість та ефективність інформаційних систем, а й забезпечити відповідність сучасним стандартам кібербезпеки. На рис. 6 наведено пропоновану модель поетапного впровадження ZTA на IT-підприємстві, яка включає в себе, у тому числі, концепції підходу DevSecOps та охоплює компоненти розширеної моделі нульової довіри ZTX [5], а саме оточуючі елементи (робочі навантаження (workloads), мережі (networks), пристрої (devices) і люди (people), які є провідниками даних і, отже, також потребують захисту), а також видимість та аналітика/аналіз (visibility and analytics), автоматизація (automation) та оркестрування/оркестрація (orchestration). Окрім цього при впровадженні ZTA необхідно враховувати дотримання організаціями вимог галузевих практик і стандартів.

Також слід відмітити, що поетапне впровадження ZTA в рамках запропонованої моделі, окрім основних процесів, передбачає виконання низки підпроцесів, які деталізують кожен процес реалізації ZTA. У табл. 3 наведено структуру цих процесів, їхній зміст у вигляді підп-

роцесів і послідовність виконання етапів, необхідних для впровадження та подальшого ефективного функціонування ZTA.

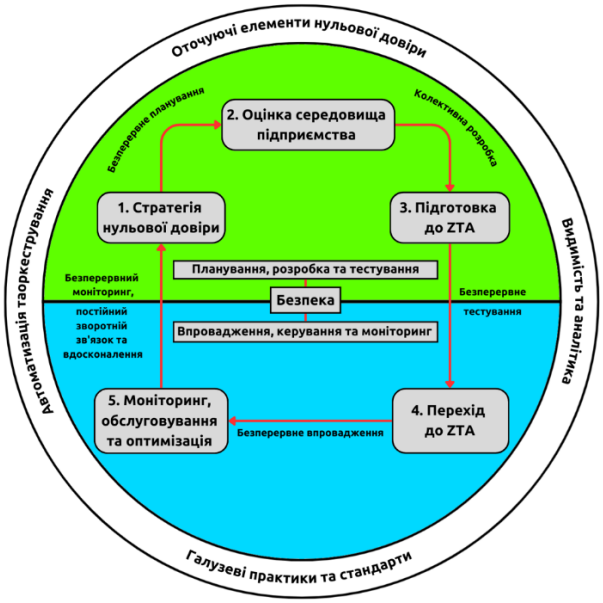

Рис. 6. Пропонована модель впровадження архітектури нульової довіри

Таблиця 3

Процеси та підпроцеси поетапного впровадження архітектури нульової довіри

Процес	Підпроцеси
Стратегія нульової довіри підприємства	Етап 1. Створення стратегії нульової довіри. Етап 2. Створення команди для впровадження ZTA.
Оцінка середовища підприємства	Етап 3. Виявлення та інвентаризація активів підприємства. Етап 4. Розробка політик доступу. Етап 5. Визначення існуючих можливостей та технологій забезпечення безпеки. Етап 6. Створення плану міграції.
Підготовка до впровадження ZTA	Етап 7. Усунення недоліків у політиках та процесах забезпечення нульової довіри. Етап 8. Підготовка пристроїв, користувачів та мережі.
Перехід до ZTA	Етап 9. Впровадження компонентів ZTA, поступове використання існуючих безпекових рішень для досягнення кінцевої мети. Етап 10. Перевірка реалізації для підтвердження підсумкових досягнень під час розгортання ZTA та виправлення виявлених помилок після впровадження.
Моніторинг, обслуговування та оптимізація ZTA	Етап 11. Забезпечення безперервного моніторингу та технічного обслуговування екосистеми нульової довіри відповідно до виявлених помилок, актуальних загроз та вимог безпеки. Етап 12. Впровадження автоматизації процесів, постійне вдосконалення та розвиток відповідно до змін характеру загроз, завдань, технологій та нормативних документів.

2.1. Стратегія нульової довіри

Першим кроком для впровадження ZTA є розробка відповідної стратегії, яка базується на принципах нульової довіри. Чітке формулювання цієї стратегії є критично важливим для успішного впровадження ZTA на підприємстві. Після її розробки необхідно досягти підтримки з боку ключових зацікавлених сторін, зокрема керівництва та кінцевих користувачів, які мають усвідомити важливість переходу до ZTA та активно сприяти цьому процесу. Крім того, для ефективного переходу до ZTA необхідно створити спеціалізовані команди, що включатимуть фахівців з впровадження рішень нульової довіри та осіб, які приймають рішення в сфері інформаційних технологій всередині підприємства. Результатом цього етапу є розробка комплексного плану переходу до ZTA, який визначатиме основні цілі та напрями впровадження ZTA для всіх учасників процесу [50].

Етап 1. Створення стратегії нульової довіри. На початковому етапі впровадження ZTA підприємство повинно сформулювати стратегічне бачення та визначити ключові цілі реалізації цього підходу. Важливим аспектом є забезпечення підтримки з боку керівництва, постачальників, партнерів та кінцевих користувачів. Основним завданням є формування єдиного розуміння необхідності переходу до ZTA, що зумовлено потребою підвищення адаптивності бізнес-процесів, оптимізації керування IT-інфраструктурою та відповідності нормативним вимогам. Окрім внутрішніх заходів, підприємство має забезпечити відповідність стандартам безпеки та нормативно-правовим вимогам, що регулюють впровадження ZTA. Це передбачає взаємодію з державними регуляторами та органами сертифікації, які встановлюють вимоги до інформаційної безпеки, а також врахування рекомендацій галузевих стандартів та міжнародних протоколів. Забезпечення ефективної комунікації з цими суб'єктами сприятиме усуненню можливих розбіжностей у трактуванні концепції ZTA та мінімізації ризиків затримки при її впровадженні [30]. Стратегічний план переходу до ZTA повинен містити комплексний аналіз поточного середовища, оцінку доступних технологічних рішень та визначення масштабу впровадження [51]. На основі цього аналізу, доцільно здійснити тестування на обмеженій частині IT-інфраструктури, що дозволить оцінити ефективність обраних рішень, виявити потенційні вразливості та сформувати оптимальний підхід до подальшого масштабування ZTA. Це також дозволить організації адаптувати ZTA відповідно до актуальних потреб та вимог підприємства [30].

Етап 2. Створення команди для впровадження ZTA. Для успішного впровадження ZTA важливим елементом є створення відповідної команди, яка забезпечить безперешкодний перехід до реалізації концепції нульової довіри. Команда повинна бути міжфункціональною, що передбачає залучення спеціалістів з різних підрозділів, таких як керування бізнес-процесами та IT. Команда повинна об'єднувати як керівників, які приймають стратегічні рішення, бізнес-аналітиків, а також технічних експертів з безпеки, зокрема які мають досвід у сфері захисту даних (включно із безпекою баз і сховищ даних), застосунків, мережі та інфраструктури, ідентифікації та керування користувачами і пристроями тощо [7, 29]. До основних завдань команди належить визначення стратегії впровадження ZTA, контроль за виконанням планів і забезпечення підтримки на всіх етапах реалізації стратегії нульової довіри. Важливим є ухвалення рішень щодо впровадження нових технологій та ініціатив, перевірка поточних рішень, визначення архітектури підприємства, а також просування технічних рішень у реальне IT-середовище. Окрім того, важливою складовою є ефективна комунікація в процесі впровадження ZTA з усіма сторонами, зокрема з користувачами, оскільки недостатнє інформування може призвести до непорозумінь і неспроможності ефективно реалізовувати концепцію нульової довіри на підприємстві. Для цього організація повинна розробити відповідний план комунікацій або провести кампанію, що забезпечить підвищення обізнаності та інформування користувачів на ранніх етапах впровадження, що сприятиме отриманню їхньої підтримки [52]. Для комунікації можна застосовувати різноманітні методи, зокрема особисті зустрічі, конференції на рівні компанії, електронну пошту, інформаційні сервіси, відео та блоги.

2.2. Оцінка середовища підприємства

Оцінка середовища є комплексним процесом при впровадженні ZTA та передбачає аналіз поточного стану підприємства, зокрема виявлення та інвентаризацію активів, розробку політик доступу, оцінку існуючих заходів безпеки, а також розробку стратегії міграції до нової архітектури. Основною метою оцінки є визначення ключових активів та ресурсів, формування деталізованого уявлення про поточний рівень захищеності підприємства, а також ідентифікація потенційних ризиків і вразливостей. Важливим компонентом цього процесу є розробка політик доступу для підтримки завдань та корпоративних сценаріїв використання, а також тестування на проникнення (penetration testing), яке дозволяє виявити слабкі місця в інфраструктурі та оцінити ефективність існуючих механізмів захисту. Результатом оцінки

середовища є створення базового плану міграції до ZTA, який визначає поточний стан підприємства та слугує основою для подальшого впровадження концепції нульової довіри.

Етап 3. Виявлення та інвентаризація активів підприємства. Першочерговим завданням команди впровадження ZTA є ідентифікація всіх активів, що використовуються в IT-середовищі підприємства. Це передбачає визначення наявних ресурсів, зокрема обладнання, ПЗ, застосунків, даних і сервісів. Для досягнення цієї мети може знадобитися впровадження спеціалізованих засобів моніторингу трафіку, які дозволяють виявити активні елементи інфраструктури та ресурси, до яких здійснюється доступ. Важливо отримати повне уявлення про всі ресурси, як локальні, так і хмарні, та провести їх систематизований облік. Це включає визначення кількості, місця розташування, рівня захисту, значущості та впливу кожного ресурсу на функціонування підприємства, адже саме вони стануть основними об'єктами, які необхідно захищати в межах ZTA. Додатково слід приділити увагу пристроям, що не належать підприємству, але можуть бути підключені до його мережевої інфраструктури або мати доступ до корпоративних ресурсів. Після складання повного переліку активів необхідно оцінити їхній поточний стан: чи відповідають вони сучасним вимогам, чи потребують оновлення, а також чи виникають у користувачів труднощі з доступом до них. Наявність неврахованих ресурсів несе ризик їхньої недостатньої захищеності в рамках концепції нульової довіри, що може зробити їх вразливими до витоку даних, несанкціонованої модифікації, видалення, відмови в обслуговуванні чи інших атак [15]. Таким чином, після проведення виявлення та інвентаризації активів наступним кроком є розробка політик доступу, які визначатимуть умови використання цих ресурсів у межах ZTA. Це забезпечить контрольоване та безпечне керування доступом відповідно до принципів найменших привілеїв та поділу обов'язків.

Етап 4. Розробка політик доступу для підтримки завдань та корпоративних сценаріїв використання. Після ідентифікації всіх ресурсів, що потребують захисту, та визначення їхнього розташування, необхідно сформулювати політики доступу в межах ZTA. Вони мають регламентувати, хто та за яких обставин отримує доступ до кожного ресурсу. Політики доступу повинні відповідати принципам найменших привілеїв і поділу обов'язків, а їх розробка має враховувати категорії користувачів, які потребують доступу, їхні посади, умови контрактів, типи пристроїв та моделі власності (наприклад, особиста, корпоративна) тощо. Усі ці фактори впливають на формування політик [15]. Дозволи на доступ можуть бути обмежені залежно від місцезнаходження особи, яка запитує доступ, часу доби або інших параметрів, які можуть додатково обмежувати доступ без втручання у роботу підприємства. Формування політик має ґрунтуватися на критичності захищених ресурсів, зокрема з урахуванням особливостей реалізації багаторівневих політик у середовищах, що використовуються для створення, розгортання та керування сучасними хмарними застосунками [53]. Однак у процесі розробки політик підприємства можуть зіткнутися з певними труднощами. Зокрема, ZTA зазвичай складається з численних компонентів, які можуть виконувати функції як PE, так і PA. В результаті політика доступу не може бути централізована в одному місці, оскільки правила можуть розподілятися між різними компонентами [15]. Наприклад, деякі з них у системах EDR, інші в системах керування ідентифікацією, обліковими даними та доступом, треті – у компоненті мережевої безпеки або захисту даних. Відсутність єдиного централізованого сховища для всіх правил може ускладнити повне розуміння політик доступу, і підтримку структурованого та узгодженого керування. Тому, щоб ефективно керувати політиками доступу, підприємство повинно не лише чітко відстежувати правила, а й розуміти, в яких саме компонентах вони визначені. З огляду на це, наступним важливим кроком є визначення наявних елементів інфраструктури, що вже виконують функції безпеки. Це дозволить підприємству інтегрувати нові політики в існуючі технологічні рішення та засоби кібербезпеки. Тому після розробки політик доступу необхідно здійснити оцінку наявних можливостей та технологій забезпечення безпеки, щоб визначити, які з них можна адаптувати чи інтегрувати в нову модель безпеки.

Етап 5. Визначення існуючих можливостей та технологій забезпечення безпеки. Якщо підприємство планує впроваджувати ZTA в абсолютно новому середовищі, не маючи попередньо створеної IT-інфраструктури чи засобів безпеки, які потребували б адаптації, цей етап можна пропустити. Однак більшість організацій не розпочинають процес впровадження ZTA з нуля, а використовують вже наявні технологічні рішення та засоби безпеки, для них важливим є врахування існуючих елементів інфраструктури, які вже виконують певні функції захисту. Як правило, підприємства мають базові засоби безпеки, такі як мережеві брандмауери та системи виявлення вторгнень, що забезпечують захист периметра. Крім того, вони часто використовують рішення для керування ідентифікацією та контролю доступу, які дозволяють автентифікувати користувачів і надавати їм відповідні права доступу на основі ідентифікаційних даних і визначених ролей. На робочих станціях, ноутбуках та/або мобільних пристроях можуть бути встановлені системи EDR, що виконують функції брандмауера, антивірусного захисту тощо. Також багато організацій використовують інструменти безпеки для ведення журналів подій, контролю конфігурацій, управління вразливостями та інших процесів, пов'язаних із забезпеченням кібербезпеки. Крім цього, в структурі підприємства, як правило, функціонує центр керування безпекою, який відповідає за моніторинг, аналіз загроз та координацію заходів реагування [15].

На даному етапі командою проводиться визначення рівня захищеності інфраструктури підприємства та виявлення вразливих місць у системі безпеки. Першим кроком на цьому етапі є оцінка існуючих заходів безпеки, яка передбачає аналіз наявних механізмів захисту для перевірки відповідності принципам нульової довіри. Підприємство має ідентифікувати та описати наявні компоненти й функціональні можливості систем безпеки, щоб визначити, які механізми захисту вже впроваджені. Далі необхідно оцінити, чи можуть ці елементи й надалі забезпечувати належний рівень безпеки в межах впровадження ZTA або ж потребують модифікації (заміни). З метою оптимізації витрат підприємство буде прагнути продовжувати використовувати або оновлювати вже наявні технології, не жертвуючи при цьому безпекою. Проте, продовження використання існуючих технологій вимагатиме від підприємства розуміння того, як існуюча система захисту буде інтегрована та взаємодіятиме з потенційними компонентами та рішеннями нульової довіри. Будь-які нові елементи, що будуть придбані спеціально для впровадження в рамках ZTA, в ідеалі повинні інтегруватися з компонентами засобів безпеки, які організація вже має та планує продовжувати використовувати [15]. Після цього проводиться аналіз розривів (gap analysis), який дозволяє оцінити поточний стан безпеки підприємства та визначити напрямки для вдосконалення [54].

Наступним кроком є проведення оцінки ризиків безпеки, що дозволяє ідентифікувати зовнішні та внутрішні загрози, а також фактичні та потенційні ризики. Цей процес включає визначення ключових активів, які потребують захисту, та розробку стратегії керування ризиками. Результати оцінки ризиків можуть бути використані для проєктування заходів для захисту, зокрема впровадження принципу найменших привілеїв, ZK та обмеження доступу до критичних ресурсів. Крім того, оцінка ризиків допомагає визначити пріоритети при впровадженні ZTA, зосереджуючись на процесах з найнижчим рівнем ризику [18, 23]. Ключовим елементом цієї оцінки є тестування на проникнення, яке дозволяє імітувати дії зловмисника з метою виявлення вразливих місць у механізмах захисту та інформаційних системах підприємства, оцінити їх рівень ефективності та визначити потенційні шляхи обходу політик нульової довіри. Його результати не лише дають змогу оцінити ефективність чинних заходів безпеки, а й виявити критичні слабкі місця, що можуть бути використані для компрометації корпоративної інфраструктури [55]. Тому інтеграція тестування на проникнення у модель розгортання ZTA є ключовим інструментом оцінки ефективності засобів захисту шляхом моделювання реальних сценаріїв кібератак.

Одним із пріоритетних завдань тестування на проникнення є виявлення вразливостей у системах контролю доступу. У ході контрольованих атак перевіряється, чи здатен зловмисник обійти механізми автентифікації або скористатися надмірними або неналежно налашто-

ваними правами доступу. Окрема увага приділяється оцінці ефективності впровадження мікросегментації, а саме проводитися моделювання бічного переміщення в мережі, що дозволяє оцінити здатність архітектури до ефективного стримування та локалізації інцидентів. Тестуванню на проникнення підлягають також системи керування ідентифікацією та контролю доступу, де перевіряються потенційні шляхи підвищення привілеїв, недоліки у механізмах автентифікації та помилки в обробці сеансів доступу. У контексті гібридних і хмарних середовищ, де ZTA реалізується між локальними та хмарними компонентами, важливо оцінити рівень безпеки при передачі даних між середовищами. Крім того, з огляду на постійну перевірку справжності/ідентифікації суб'єкта, а також виконання автентифікації та авторизації суб'єктів в рамках ZTA, тестуванню на проникнення підлягають кінцеві пристрої та застосунки, включно з виявленням вразливостей, пов'язаних із застарілим ПЗ або неправильними налаштуваннями.

З іншого боку, слід мати на увазі, що впровадження тестування на проникнення в ZTA супроводжується низкою викликів. Зокрема, динамічні політики безпеки, які адаптуються залежно від поведінки користувача та контексту, ускладнюють створення постійної методології тестування. Мікросегментація й посилений контроль доступу обмежують можливості традиційного тестування на проникнення, яке покладається на бічне переміщення, а засоби безперервного моніторингу з підтримкою ШІ можуть розцінювати дії при тестуванні як реальну загрозу, активуючи автоматизовані механізми реагування, що перешкоджає проведенню тестування на проникнення. Ще одним викликом є інтеграція тестування на проникнення в процеси DevSecOps протягом циклу розгортання ZTA, а команда тестування на проникнення повинна тісно співпрацювати з командою впровадження ZTA. Тому, з метою усунення зазначених викликів, варто дотримуватися низки запропонованих практик. Передусім, необхідно чітко визначати цілі тестування, які повинні узгоджуватися зі специфікою архітектури, а саме перевіркою механізмів автентифікації, ефективності сегментації мережі, політик контролю доступу, налаштувань безпеки гібридної або хмарної інфраструктури. При цьому варто застосовувати механізми ШІ та засоби автоматизації для ефективного аналізу великих обсягів даних та моделювання сценаріїв атак. В свою чергу, використання підходів «червоної команди» (red team) і «блакитної команди» (blue team) у форматі взаємодії (purple team) дає змогу не лише моделювати реальні кібератаки, але й узгоджено перевіряти ефективність заходів безпеки. Також, особливу увагу слід приділити перевірці механізмів керування доступом, де ключовими аспектами при тестуванні на проникнення є потенційні методи обходу MFA, ризики перехоплення сеансів користувачів, перевірка політики паролів, а також вразливість до атак соціальної інженерії. У цьому контексті важливо враховувати, що взаємодія в межах ZTA дедалі частіше реалізується через API-з'єднання та хмарні провайдери. Відтак, актуальним стає тестування механізмів автентифікації для API, виявлення неправильних налаштувань хмарних сервісів, а також оцінка відповідності вимогам галузевих стандартів безпеки (наприклад, NIST 800-207, CIS Benchmarks). Однак ZTA передбачає наявність загроз не лише ззовні, тому важливим елементом є моделювання дій інсайдера. Зокрема це можуть бути спроби ексфільтрації (несанкціонована передача) даних, підвищення привілеїв чи зловживання легітимними обліковими записами. Тому, з огляду на постійний розвиток концепції нульової довіри та ускладнення цифрового середовища підприємств, стратегії тестування на проникнення повинні регулярно оновлюватися. Це дає змогу своєчасно виявляти нові вектори атак і підтримувати належний рівень кібербезпеки підприємства.

Таким чином, проведення тестування на проникнення має ключову роль при впровадженні ZTA та дозволяє не лише оцінити ефективність наявних засобів захисту та дотримання принципів нульової довіри, але й виявити слабкі місця, що можуть бути використані для компрометації IT-інфраструктури, а також встановити пріоритети для вдосконалення реалізації ZTA. Такий підхід забезпечує обґрунтовану й цілеспрямовану оптимізацію політик безпеки, орієнтовану на запобігання несанкціонованому доступу та зміцнення загальної кіберстійкості підприємства. В свою чергу дані, отримані в результаті аналізу на даному етапі

встановлюють, на якій стадії впровадження ZTA перебуває підприємство: чи воно функціонує за традиційною моделлю безпеки, чи вже інтегрує окремі елементи нульової довіри, чи наближається до повного її впровадження, що передбачає застосування передових технологій, зокрема автоматизованих систем аналізу загроз на основі ШІ [26, 56]. Отримані результати інтегруються у загальний план керування ризиками та слугують основою для формування стратегії поступового переходу до концепції нульової довіри. Оцінка поточного стану підприємства є невіддільним етапом підготовки до впровадження ZTA, оскільки вона дозволяє виявити прогалини в наявних механізмах захисту, визначити рівень ризиків та встановити пріоритетні напрями їх мінімізації. На основі отриманих результатів та оцінки формується детальний план міграції до ZTA, який передбачає модернізацію інфраструктури, перегляд та вдосконалення політик безпеки, а також реалізацію комплексних заходів для досягнення необхідного рівня захищеності корпоративної інформаційної системи.

Етап 6. Створення плану міграції. Процес впровадження ZTA передбачає розробку плану міграції, який підприємство використовуватиме для реалізації ZTA. Перед початком впровадження ZTA необхідно здійснити детальний аналіз доступних рішень і технологій, що відповідають вимогам підприємства та концепції нульової довіри [53]. Вибір постачальників має ґрунтуватися на всебічному вивченні технічних вимог ZTA, що забезпечить відповідність придбаних рішень встановленим критеріям. Одним із ключових аспектів вибору технологій є забезпечення сумісності ПЗ, що дозволить уникнути ефекту «прив'язки до постачальника». Для запобігання цій проблемі необхідно враховувати можливості адаптації послуг, зокрема наступні параметри: якість обслуговування (Quality of Service) та угода про рівень послуг (Service-Level Agreement). Це сприятиме гнучкості у подальшій експлуатації та модернізації ZTA. Розробка плану міграції передбачає структурований розподіл завдань на етапи та визначення їх пріоритетності відповідно до потреб підприємства [57]. Ефективне планування дає змогу раціонально розподілити ресурси, що сприяє зменшенню витрат та оптимізації часових рамок при впровадження ZTA. Крім того, необхідно створити тестові плани та план оцінювання ефективності впровадження ZTA, що забезпечить можливість об'єктивного аналізу успішності міграції. Для досягнення швидких результатів підприємство може використовувати підхід, заснований на конкретних сценаріях використання (use-case), що дозволить вирішити окремі проблеми за допомогою невеликих команд та обмеженого бюджету.

2.3. Підготовка до впровадження архітектури нульової довіри

Підготовка до впровадження ZTA вимагає комплексного та послідовного підходу, що охоплює пристрої, користувачів і мережеву інфраструктуру. Перш за все необхідно усунути недоліки у політиках та процесах забезпечення нульової довіри. Це здійснюється через застосування підходу, заснованого на оцінці ризиків і цінності даних, що дозволяє оптимізувати існуючі політики доступу та забезпечити їх відповідність принципам ZTA. Виявлені недоліки в процесах і політиках потребують коригування для забезпечення максимальної ефективності та безпеки. Після вдосконалення політик і процесів наступним кроком є підготовка пристроїв, користувачів та мережі до інтеграції з ZTA. На цьому кроці передбачається налаштування відповідних компонентів інфраструктури, що дозволить безперешкодно реалізувати контроль доступу згідно з новими політиками і підвищити загальний рівень безпеки організації. Таким чином, процес підготовки до впровадження ZTA можна поділити на такі етапи.

Етап 7. Усунення недоліків у політиках та процесах забезпечення нульової довіри шляхом застосування підходу, заснованого на оцінці ризиків та цінності даних. Після того як буде визначено перелік ресурсів, що потребують захисту, а також оцінено середовище підприємства та наявні засоби безпеки, наступним кроком є планування технології захисту доступу. Вона передбачає ухвалення рішень щодо визначення рівня захисту кожного ресурсу та сегментації інфраструктури. Ефективне впровадження технології захисту доступу ґрунтується на підході, орієнтованому на ризики: критично важливі ресурси повинні бути ізольовані у

власних зонах довіри, де контроль здійснюється через PEP, тоді як менш важливі ресурси можуть розміщуватися у одній зоні довіри. Для успішного захисту IT-підприємства, необхідно оцінити рівень ризику для кожного ресурсу та надати їм рівні. Оцінка включає аналіз ймовірності виникнення загрози та потенційного збитку, який вона може спричинити для підприємства. Після документування ризиків стає зрозуміло, які ресурси є найбільш критично важливими для роботи підприємства та які вразливості вони мають. Подібний підхід відповідає принципам дії у межах системи керування ризиками (Risk Management Framework), оскільки впровадження ZTA є насамперед процесом зниження ризиків для бізнес-функцій підприємства [15].

На етапі розробки технології захисту доступу підприємству слід визначити, які PEP відповідатимуть за захист кожного ресурсу, а також які допоміжні технології будуть залучені до ухвалення рішень про доступ. Початковий стан мережі може не передбачати сегментації, фактично до впровадження ZTA, коли підприємство все ще покладається на захист на основі периметра, таку технологію можна представити як централізований захист усіх ресурсів підприємства за допомогою однієї PEP, наприклад, брандмауер на периметрі. Проте поступове впровадження ZTA передбачає сегментування інфраструктури на дрібніші частини, що дозволяє обмежити вплив потенційних атак або порушень та спростити моніторинг мережевого трафіку. Захист доступу має бути багаторівневим і охоплювати контроль на рівні застосунків, вузлів і мережевої інфраструктури. Водночас ефективність реалізованих політик і заходів безпеки значною мірою залежить від готовності підприємства до їхнього впровадження. Наступним кроком у цьому процесі є підготовка пристроїв, користувачів та мережі до роботи в умовах нульової довіри.

Етап 8. Підготовка пристроїв, користувачів та мережі. Для забезпечення безпечного функціонування пристроїв у межах корпоративної мережі необхідно впровадити систему керування обліком пристроїв (Device Inventory Management), яка дозволяє вести централізований облік усіх пристроїв, підключених до корпоративного середовища [24]. Це дає змогу контролювати перелік активних пристроїв і забезпечувати доступ лише тим, які відповідають встановленим вимогам безпеки [3, 26]. Крім того, усі пристрої повинні відповідати встановленим стандартам безпеки, мати необхідне ПЗ для захисту від кібератак та перебувати під постійним моніторингом для своєчасного виявлення потенційних загроз [58]. З метою запобігання несанкціонованому доступу до інформаційних активів підприємства необхідно впровадити механізми оцінки відповідності пристроїв (compliance check). Це дозволить визначати пристрої з високим рівнем ризику та обмежувати їхній доступ до критично важливих ресурсів. Важливим аспектом є облік як корпоративних, так і особистих пристроїв (BYOD), що забезпечує гнучкість у роботі співробітників, водночас знижуючи ризики за рахунок використання механізмів керування мобільними пристроями (Mobile Device Management) та мобільністю підприємства (Enterprise Mobility Management).

Ідентифікація та автентифікація користувачів є фундаментальним аспектом безпеки в рамках ZTA. Для цього організація повинна створити централізовану базу даних облікових записів, що містить актуальну інформацію про користувачів, їхні ролі та рівень доступу [24]. Дотримання принципу найменших привілеїв забезпечує мінімізацію можливих загроз, пов’язаних із компрометацією облікових записів. Користувачі можуть бути класифіковані за категоріями, а саме: співробітники підприємства, клієнти, партнери та адміністратори, які мають розширені права для налаштування доступу [3]. Для захисту облікових записів слід застосовувати MFA, що значно знижує ризик несанкціонованого доступу. Додаткові заходи безпеки включають використання механізмів керування привілейованими обліковими записами (Privileged Identity Management) та PAM, які унеможливлюють використання підвищених привілеїв у разі компрометації облікового запису [50].

Корпоративна мережа повинна бути структурована таким чином, щоб забезпечити захищений обмін даними та мінімізувати потенційні загрози. Одним із важливих підходів є мікросегментація мережі, що ґрунтується на створенні ізольованих сегментів із контрольованим

обміном даними між ними. Це дозволяє обмежити розповсюдження можливих атак і забезпечити доступ до критично важливих ресурсів лише тим користувачам і пристроям, які мають на це відповідні дозволи [59]. Окрім мікросегментації, важливим аспектом є забезпечення контрольованого доступу шляхом застосування шлюзів безпеки, які фільтрують увесь вхідний і вихідний трафік. Для підвищення рівня безпеки слід впровадити механізми розширеного моніторингу мережевої активності, що включає виявлення аномальної поведінки користувачів та пристроїв, а також аналіз трафіку в реальному часі. Повна видимість активів у мережі та дотримання встановлених стандартів кібербезпеки є критично важливими умовами ефективного впровадження ZTA. В свою чергу, всі запити на доступ до ресурсів повинні проходити через механізми ідентифікації та авторизації, що гарантує відповідність кожної сесії вимогам безпеки. Це сприяє створенню динамічного механізму керування доступом, який адаптується до змін у середовищі загроз та поточних бізнес-процесів підприємства [3].

2.4. Перехід до архітектури нульової довіри

Впровадження ZTA вимагає комплексного підходу, що вимагає ретельної та поетапної підготовки. Цей перехід охоплює всі аспекти цифрового середовища підприємства, включаючи користувачів, пристрої та мережеву інфраструктуру. Основним завданням на цьому етапі є забезпечення безперервності бізнес-процесів підприємства та мінімізація впливу змін на роботу користувачів. Під час переходу до ZTA необхідно поступово адаптувати застосунки та сервіси, забезпечуючи їхню сумісність із сучасними механізмами контролю доступу та протоколами безпеки. Важливим є зменшення залежності від традиційних рішень на основі периметру, таких як VPN, шляхом надання доступу лише для тих користувачів, хто потребує цього для виконання своїх завдань. Усі застосунки та сервіси мають працювати через визначені шлюзи, а їхнє використання контролюватися відповідно до встановлених політик доступу. Також необхідно реалізувати комплексний моніторинг мережевого трафіку, аналіз активності користувачів і пристроїв, щоб забезпечити відповідність діям заданим правилам безпеки. Подальші кроки передбачають оцінку ефективності реалізованих заходів та адаптацію політик безпеки на основі отриманих результатів. Виявлені проблеми потребують коригування та повторного тестування, щоб гарантувати стабільність та функціональність системи. Після підтвердження стабільної роботи впроваджених рішень, впровадження ZTA розширюється на всю інфраструктуру підприємства, забезпечуючи поступову інтеграцію сучасних механізмів контролю доступу та виведення з експлуатації застарілих рішень. На цьому етапі починається впровадження ключових компонентів ZTA. Далі здійснюється перевірка реалізації, оцінка підсумкових досягнень та виправлення можливих виявлених недоліків для остаточного завершення процесу переходу до ZTA.

Етап 9. Впровадження компонентів ZTA, поступове використання існуючих безпекових рішень для досягнення кінцевої мети. Щойно підприємство досягне чіткого розуміння існуючого середовища з точки зору ресурсів, які потребують захисту, та вже розгорнутих засобів безпеки, сформулює політики доступу, які підходять для підтримки його завдань та бізнес-показників, розробить технологію захисту доступу із зазначенням рівня деталізації, з яким захищатиметься доступ до різних ресурсів і допоміжних технологій, які будуть використовуватись у PDP, підприємство може безпосередньо розпочати поступове впровадження ZTA [15].

Зважаючи на те, що нині існують різні моделі розгортання нульової довіри [15], важливо визначити, яка саме архітектура найбільш підходить для конкретного IT-підприємства. Наприклад, під час вибору міжмережевих екранів із PDP слід враховувати функціональні ролі брандмауерів як елементів інфраструктури – шлюзів (PEP), які відіграють ключову роль у реалізації детальних мережевих політиках та політиках рівня ідентифікації. Відповідно до рекомендацій NIST [53], можна виділити кілька типів шлюзів, що забезпечують функціональність у межах ZTA: вхідний шлюз (Ingress gateway) регулює вихідні запити застосунків за межі кластеру/групи, контролюючи імена, сертифікати, порти, протоколи та кінцеві точки, які обслуговуються за межами кластера; вихідний шлюз/шлюз виходу (Egress gateway) керує

взаємодією застосунків у межах кластеру/групи із зовнішнім середовищем, може використовуватися для традиційної фільтрації та реєстрації вихідних повідомлень, як проксі Squid, але також може реалізовувати політики на основі ідентифікації, дозволяючи або обмежуючи обмін обліковими даними; граничний/крайовий шлюз (Edge gateway) працює на межі між мережею та вхідним шлюзом, оптимізуючи трафік, забезпечуючи балансування навантаження між групами або вузлами, також використовується для переривання зовнішнього трафіку та підвищення стійкості до відмов на рівні інфраструктури; окрім цього, є Sidecar gateway, який функціонує поруч із кожним екземпляром застосунка, перехоплюючи весь вхідний і вихідний трафік та обробляючи внутрішні комунікації між сервісами в інфраструктурі.

Ключовими аспектами, які підприємство має враховувати при розгортанні ZTA, є ідентифікація, автентифікація та авторизація суб'єктів, а також перевірка відповідності кінцевих пристроїв встановленим політикам. Враховуючи, що прийняття та виконання рішень щодо доступу є основними складовими ZTA, підприємству доцільно використовувати існуючі або нові рішення керування ідентифікацією, обліковими даними та доступом (Identity, Credential, Access Management – ICAM) як базовий компонент реалізації ZTA. Важливим кроком є впровадження MFA для всіх користувачів та інтеграція EDR (або аналогічне рішення, що може оцінювати стан пристрою) із системою ICAM. Початкова ZTA, що базується на цих компонентах, зможе забезпечити контрольовану ідентифікацію та авторизацію суб'єктів, а також стан і відповідність вимогам кінцевих пристроїв, що запитують, як основу для прийняття рішень про доступ, що згодом можна розширити додатковими компонентами та функціями безпеки для задоволення більшої кількості вимог ZTA. Подальший розвиток ZTA залежить вже, безпосередньо, від пріоритетів підприємства. Якщо основним завданням є захист даних, першочергово слід впроваджувати компоненти безпеки даних. Якщо ж акцент робиться на виявленні аномалій з урахуванням поведінки, варто встановити рішення для моніторингу і систему аналізу на основі ШІ. ZTA має розвиватися поступово, включаючи додаткові допоміжні компоненти, функції та можливості, щоб крок за кроком забезпечити її повну функціональність. При цьому варто зазначити, що розгортання ZTA може супроводжуватися складнощами (протидія змінам), зокрема пов'язаними з людським фактором. Опір змінам може виникати через технічні упередження, культуру, емоційну орієнтацію на існуючі інструменти, архітектуру безпеки або процеси компанії [30]. Ця проблема може здаватися незначною у порівнянні з фінансовими та апаратними складовими, однак це може викликати серйозні проблеми із впровадженням. Щоб подолати ці труднощі, необхідно інвестувати у навчання персоналу, підвищуючи їх кваліфікацію та рівень обізнаності щодо принципів нульової довіри та методів їх реалізації. Важливим є розуміння того, що ефективне впровадження ZTA безпосередньо залежить від рівня підготовки користувачів та їхнього усвідомлення переваг нової архітектури, знання основних принципів нульової довіри, які застосовуються до ситуації, а також методів, необхідних для забезпечення дотримання цих принципів.

Завершальним етапом впровадження є перевірка реалізованої архітектури, що дозволить підтвердити досягнення запланованих цілей та здійснити корекцію виявлених недоліків після впровадження ZTA.

Етап 10. Перевірка реалізації для підтвердження підсумкових досягнень під час розгортання ZTA та виправлення виявлених помилок після впровадження. Для оцінки успішності впровадження ZTA та ефективності його роботи мають застосовуватися плани тестування та відповідні метрики. Вибрані для тестування сценарії використання повинні відповідати тим, які найбільш точно відображають повсякденний доступ користувачів підприємства до його ресурсів. В ідеалі підприємство може створити набір тестів, які можна використовувати для перевірки можливостей у рамках ZTA не лише перед розгортанням кожної нової функціональності в процесі поступового впровадження ZTA, а й на основі регулярного тестування після завершення розгортання ZTA. Наприклад, можуть проводитися тестування на проникнення, перевірка стійкості до викрадення даних, протистояння фішинговим атакам, фальсифікації даних тощо [15]. Водночас підприємство повинно передбачити механізми або канали для

усунення можливих помилок, що можуть виникнути під час експлуатації системи. Наприклад, можуть бути впроваджені засоби самостійного вирішення типових проблем користувачами шляхом використання покрокових інструкцій або керівництв, а також організовані інформаційні сервіси, які надаватимуть відповіді на поширені питання (Frequently Asked Questions – FAQ). Для своєчасного інформування про оновлення, пов'язані з впровадженням ZTA, та можливі тимчасові зміни в доступі до ресурсів, може бути налаштована система електронних сповіщень для користувачам. У разі виникнення складніших (не типових) проблем команда впровадження ZTA повинна бути готова оперативно реагувати, аналізувати причини збоїв та забезпечувати швидке усунення несправностей, мінімізуючи їх вплив на користувачів. Для цього члени команди мають пройти відповідне навчання, щоб ефективно допомагати користувачам у разі перебоїв і сприяти швидкому відновленню роботи. Після того як команда впровадження підтвердить стабільне функціонування всіх компонентів ZTA та усуне виявлені недоліки, процес впровадження переходить до наступного етапу, а саме безперервного моніторингу та обслуговування ZTA, що дозволяє забезпечити її довгострокову ефективність та адаптивність до нових викликів.

2.5. Моніторинг, обслуговування та оптимізація архітектури нульової довіри

Ефективне функціонування підприємства в рамках ZTA передбачає безперервний моніторинг і технічне обслуговування, що забезпечує контроль за станом системи, оцінку її продуктивності та відповідності вимогам безпеки. Моніторинг ZTA спрямований на досягнення повної прозорості мережевої активності, своєчасного виявлення потенційних загроз, забезпечення стабільності роботи всіх компонентів та визначення необхідності їхнього технічного обслуговування. У цьому контексті особливого значення набуває впровадження автоматизації процесів, а також постійне вдосконалення та розвиток архітектури відповідно до змін характеру загроз, завдань, технологій та нормативних документів. Здатність ZTA до динамічного реагування на зміни у середовищі функціонування, а також на зовнішні та внутрішні загрози є ключовим чинником не тільки підтримки її ефективності, але й її здатності до адаптації та збереження належного рівня безпеки в умовах динамічного кіберсередовища.

Етап 11. Забезпечення безперервного моніторингу та технічного обслуговування екосистеми нульової довіри відповідно до виявлених помилок, актуальних загроз та вимог безпеки. Після впровадження ZTA необхідно здійснювати безперервний моніторинг та технічне обслуговування екосистеми нульової довіри відповідно до виявлених вразливостей, актуальних загроз і встановлених вимог безпеки. Це передбачає контроль доступності мережевих сервісів, моніторинг мережевого трафіку в режимі реального часу, а також регулярну перевірку відповідності системи чинним стандартам безпеки [29, 60]. Окрім цього, необхідним є систематичне відстеження стану всієї IT-інфраструктури підприємства, зокрема її критичних компонентів, що забезпечують функціонування ZTA. В свою чергу, моніторинг відповідності нормативним вимогам включає проведення регулярного сканування вразливостей, виявлення потенційних витоків даних і аналіз стану реалізованих політик безпеки. Використання сучасних аналітичних інструментів (із використанням ШІ) сприяє поглибленому аналізу подій у межах ZTA, що дає змогу своєчасно виявляти аномалії та підвищувати рівень кіберзахисту. Для ефективної інтеграції таких засобів необхідно оцінювати їхню відповідність логічній архітектурі системи та забезпечувати їхнє оптимальне розміщення в межах інфраструктури підприємства [27, 61]. У разі оновлення засобів аналітики перевагу слід надавати рішенням, які сумісні з принципами нульової довіри та можуть бути інтегровані у вже функціонуючу екосистему без порушення її стабільності та функціональності.

Оцінка ефективності безпеки після впровадження ZTA є також важливим аспектом в рамках моніторингу та забезпечення безперервного функціонування ZTA. Для цього проводиться аналіз впливу впроваджених механізмів на робочі процеси та визначення їх ефективності у запобіганні кіберзагрозам [62]. Одним із ключових показників ефективності є частота виникнення інцидентів безпеки та їхній вплив на функціонування системи та роботу корис-

тувачів. Після впровадження ZTA кількість таких інцидентів має зменшитися, а також має знизитися їхній вплив на бізнес-процеси. Наприклад, можна відстежувати зменшення часу простою критичних сервісів через кіберінциденти або скорочення кількості випадків компрометації облікових записів. Крім того, важливим аспектом є оцінка навантаження на IT-відділ, що включає аналіз частоти звернень користувачів щодо проблем із доступом, часу, що витрачається на ручні перевірки та обробку сповіщень безпеки, а також кількості запитів, пов'язаних із відновленням доступу до систем. Ефективна робота ZTA сприяє автоматизації рутинних операцій безпеки та мінімізації потреби у ручному втручанні. Оцінка рівня впровадження MFA також є важливим показником ефективності: слід аналізувати відсоток працівників, які регулярно використовують MFA, а також випадки труднощів з автентифікацією через невідповідність політикам безпеки. Додаткові метрики включають кількість запитів на автентифікацію, частку співробітників, що використовують єдиний вхід (Single sign-on – SSO), динаміку використання корпоративних застосунків, а також кількість пристроїв, застосунків і сервісів, що відповідають політикам безпеки. Оптимізація ресурсів безпеки передбачає зменшення кількості інструментів, що виконують однакові функції, скорочення потреби у їх складній ручній інтеграції, а також зниження часу, витраченого на обробку хибнопозитивних (false positive) сповіщень. Використання аналітичних інструментів на основі ШІ в таких випадках дозволяє зменшити рівень помилкових сповіщень, а також своєчасно виявляти аномальні шаблони поведінки користувачів, пристроїв, мережевого трафіку та реагувати на реальні загрози. Це, у свою чергу, сприяє стабільному та ефективному функціонуванню ZTA, забезпечуючи високий рівень кіберзахисту без надмірного впливу на бізнес-процеси.

Етап 12. Впровадження автоматизації процесів, постійне вдосконалення та розвиток відповідно до змін характеру загроз, завдань, технологій та нормативних документів. Після того як ZTA буде розгорнута та буде вважатися завершеною, екосистема нульової довіри повинна продовжувати адаптуватися до умов, що змінюються. Проведена оцінка ефективності ZTA використовується для визначення подальших заходів щодо її модернізації. Якщо технологічні компоненти, що використовуються в ZTA, застарівають, їх слід замінити. І навпаки, якщо з'являються нові інноваційні технології, підприємство повинне розглянути можливість їх інтеграції в існуючу ZTA, щоб скористатися перевагами нових засобів захисту, методів та механізмів, які можуть підвищити загальний рівень безпеки підприємства [15]. Також слід враховувати, що здатність ZTA до ефективного функціонування значною мірою залежить від рівня автоматизації механізмів керування загрозами, що, у свою чергу, передбачає використання технічних рішень, спрямованих на зменшення використання ручних операцій і впровадження механізмів автоматизованого реагування. Автоматизація та оркестрування процесів безпеки також забезпечує підвищення точності виявлення атак і скорочення часу реагування на інциденти, що зумовлює необхідність інтеграції відповідних рішень у систему керування безпекою, а також відіграє ключову роль у забезпеченні безперервного вдосконалення ZTA. Завдяки автоматизованому моніторингу інфраструктури, аналізу загроз у реальному часі та адаптивному оновленню політик безпеки підприємства можуть оперативно реагувати на зміни у сфері кіберзахисту. У цьому контексті інтеграція сучасних систем безпеки для оркестрації, автоматизації та реагування (Security Orchestration, Automation, and Response – SOAR) у поєднанні з системою керування інформацією та подіями безпеки (Security Information and Event Management – SIEM) є ефективним рішенням для підвищення рівня безпеки. SOAR забезпечує централізоване керування інцидентами, автоматизацію при аналізі загроз і координацію дій між різними системами безпеки, що дозволяє мінімізувати затримки в реагуванні та зменшити навантаження на команди безпеки. SOAR-системи у поєднанні зі ШІ та машинним навчанням, демонструють значний потенціал у виявленні, пом'якшенні та запобіганні кіберзагрозам. Ось чому постачальники даних інструментів намагаються інтегрувати алгоритми ШІ та машинного навчання для підвищення ефективності команд безпеки [63]. Іншими словами, використання сучасних підходів до автоматизації та оркестрування проце-

сів безпеки дозволяє підприємствам не лише підтримувати стабільність роботи ZTA, а й досягати високого рівня адаптивності до змін у сфері кіберзахисту [60, 61].

Надалі, якщо цілі підприємства в сфері безпеки змінюються, або внаслідок зміни завдань, або внаслідок змін у нормативних документах, може знадобитися зміна політик та самої ZTA, щоб найкраще відповідати новим цілям. Тобто в рамках цього безперервного процесу валідації та вдосконалення підприємства повинні забезпечити контроль актуальності політик безпеки, технології та топології сегментації мережі, постійний автоматизований моніторинг стану мережі та іншої IT-інфраструктури, щоб переконатися, що вони залишаються ефективними. Саме автоматизація процесів безпеки дозволяє забезпечити безперервну перевірку та вдосконалення архітектури ZTA, знижуючи вплив людського фактору та забезпечуючи ефективність роботи екосистеми нульової довіри.

Наприкінці, хочеться зазначити, що розгортання та впровадження ZTA є складним, тривалим і багатоетапним процесом, який потребує ретельного аналізу та кропіткої роботи для досягнення рішень високої якості у забезпеченні безпеки IT-підприємства. Незважаючи на те, що основні принципи ZTA сьогодні вже вважаються визначеними, питання їхнього практичного впровадження залишається відкритим. Насамперед складнощі виникають відносно того, як узгодити та інтегрувати різні технологічні рішення з вимогами ZTA [64]. Тому важливим напрямом подальших досліджень є розробка технічних методів ефективного та узгодженого розгортання компонентів безпеки у межах вимог ZTA. У майбутньому необхідно більш детально дослідити підходи до впровадження таких компонентів, як мікросегментація, механізми автентифікації та системи керування доступом. Це дозволить розробляти більш ефективні способи інтеграції технологій та підвищити загальний рівень захищеності інфраструктури підприємства. Крім того, слід звернути увагу ще на один актуальний виклик – адаптацію ZTA до хмарних середовищ, оскільки сучасні підприємства все частіше використовують комбіновані архітектури, що поєднують локальні та хмарні сервіси. Такий підхід створює додаткові ризики, пов’язані з крадіжкою ідентифікаційних даних та витоками інформації. Тому також перспективним напрямом досліджень слід вважати – удосконалення методів інтеграції ZTA з хмарною інфраструктурою, зокрема, впровадження механізмів контролю доступу до ресурсів, орієнтованих на ідентифікаційні (identity-centric) та динамічні дані у хмарному середовищі.

Висновки

1. Відповідно до сучасних викликів, парадигма безпеки «нульової довіри» є оптимальним та ефективним підходом для захисту інформаційних систем цифрових підприємств від новітніх загроз. Дана концепція забезпечує безпечний доступ до корпоративних ресурсів з будь-якого місця та у будь-який час.

2. Існуючі рішення побудови систем на основі ZTA та досвід їх використання свідчать про істотні переваги нової концепції перед традиційними архітектурами, орієнтованими на захист по периметру. Проте, впровадження ZTA є не просто повною заміною технологічних процесів або інфраструктури IT-підприємства, а реалізацією плану кібербезпеки, що використовує концепцію нульової довіри та охоплює планування робочих процесів, політики доступу та зв’язки логічних компонентів.

3. Будь-яке підприємство може застосовувати принципи нульової довіри для підвищення рівня безпеки, незалежно від структури чи масштабу. В роботі розглянуті деякі рекомендації щодо практичного впровадження ZTA, з урахуванням можливих сценаріїв, викликів і оптимальних підходів до інтеграції принципів нульової довіри в корпоративне середовище IT-підприємства.

4. Враховуючи організаційні та технічні виклики, а також вимоги щодо розгортання ZTA, в даній роботі запропонована модель впровадження ZTA. Для її ефективної реалізації запропоновано п’ять основних процесів: 1) стратегія нульової довіри, 2) оцінка середовища підприємства, 3) підготовка до впровадження ZTA, 4) перехід до ZTA, 5) моніторинг, обслу-

говування та оптимізація ZTA. Важливими складовими пропонованої моделі поетапного впровадження ZTA на IT-підприємстві є концепція підходу DevSecOps та компоненти розширеної моделі нульової довіри ZTX. Окрім цього при впровадженні ZTA, запропонована модель враховує дотримання вимог галузевих практик і стандартів.

5. Представлені в роботі результати покликані допомогти спеціалістам з безпеки використати надані рекомендації щодо практичного впровадження ZTA на своїх IT-підприємствах відповідно до запропонованої моделі. Встановлено, що подальші дослідження доцільно зосередити на розробці технічних методів розгортання компонентів безпеки у межах вимог ZTA, інтеграції ZTA з хмарною інфраструктурою та більш детальному аналізі підходів впровадження таких компонентів, як мікросегментація, механізми автентифікації та системи керування доступом.

6. Запропонована модель впровадження ZTA може слугувати орієнтиром для ефективного переходу до ZTA в сучасних цифрових підприємства, а її використання відкриває значні перспективи для розвитку більш надійних та масштабованих систем захисту інформаційних ресурсів IT-підприємства, що є надзвичайно актуальним у сучасному цифровому кіберпросторі.

Список літератури:

1. Marsh S.P. Formalising Trust as a Computational Concept. Department of Computing Science and Mathematics University of Stirling. 1994. 184 p.
2. Welborn R., Kasten V. The Jericho principle: how companies use strategic collaboration to find new sources of value. John Wiley & Sons. 2003. 288 p.
3. Ward R., Beyer B. Beyondcorp // A new approach to enterprise security. 2014. 39(6). P. 6–11.
4. Gilman E., Barth D. Zero Trust Networks: Building Secure Systems in Untrusted Networks. 2017. 315 p.
5. Cunningham C., Balaouras S., Barringham B., Dostie P. The Zero Trust eXtended (ZTX) Ecosystem. Extending Zero Trust Security Across Your Digital Business. Forrester Research, Inc. Cambridge, MA. 2018. URL: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf.
6. Fisher B. Forrester's Zero Trust or Gartner's Lean Trust? 2019. URL: https://blogs.cisco.com/security/forresters-zero-trust-or-gartners-lean-trust.
7. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // NIST Special Publication 800-207. 2020. https://doi.org/10.6028/NIST.SP.800–207.
8. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.
9. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Огляд існуючих моделей та основних принципів нульової довір // Радіотехніка. 2024. Вип. 217. С. 39–54. https://doi.org/10.30837/rt.2024.2.217.03.
10. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History // Wired. (2018). URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.
11. Yampolskiy R., Spellchecker M. Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures // arXiv preprint arXiv:1610.07997. 2016. 12 p. https://doi.org/10.48550/arXiv.1610.07997.
12. Chen B., Qiao S., Zhao J., Liu D., Shi X., Lyu M., Chen H., Lu H., Zhai Y. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture // IEEE Internet of Things Journal. 8(13). 2020. P. 10248–10263. https://doi.org/10.1109/JIOT.2020.3041042.
13. MarketsandMarkets. Zero Trust Security Market. (2024). URL: https://marketsandmarkets.com/PressReleases/zero-trust-security.
14. Bertino E. Zero Trust Architecture: Does It Help? // IEEE Security & Privacy. 2021. 19(05). P. 95–96. https://doi.org/10.1109/MSEC.2021.3091195.
15. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Архітектура нульової довіри: проблеми та рекомендації щодо успішного впровадження // Радіотехніка. 2024. Вип. 218. С. 7–34. https://doi.org/10.30837/rt.2024.3.218.01.
16. Cunningham C., Holmes D., Pollard J. The eight business and security benefits of zero trust // Forrester Research, Inc. 2019. URL: https://www.forrester.com/report/the-eight-business-and-security-benefits-of-zerotrust/RES134863.
17. Fernandez E. B., Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA) // Computer Standards & Interfaces. 2024. Vol. 89. 103832. https://doi.org/10.1016/j.csi.2024.103832.
18. Teerakanok S., Uehara T., Inomata A. Migrating to Zero Trust Architecture: Reviews and Challenges // Security and Communication Networks. 2021. Vol. 6. P. 1–10. https://dx.doi.org/10.1155/2021/9947347.
19. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture // IEEE Access. 2023. Vol. 11. P. 19487–19511. https://10.1109/ACCESS.2023.3248622.

20. Ali B., Hijjawi S., Campbell L. H., Gregory M. A., Li S. A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing // Security and Communication Networks. 2022. P. 1–14. https://doi.org/10.1155/2022/3178760.

21. Haber M. J. Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations, 2nd ed. New York, NY, USA: Apress. 2020. 384 p.

22. Foltz K. E., Simpson W. R. Zero Trust Technology Integration Issues. Institute for Defense Analyses. 2021. P. 34. URL: https://www.jstor.org/stable/resrep34846.

23. Bertino E., Brancik K. Services for Zero Trust Architectures – A Research Roadmap // IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 2021. P. 14–20. https://doi.org/10.1109/ICWS53863.2021.00016.

24. CISCO. From MFA to Zero Trust: A Five-Phase Journey to Securing the Federal Workforce. 2021. URL: https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/zero-trust/mfa-zero-trust-five-phase-journey-securing-workforce.pdf.

25. Osborn B., McWilliams J., Beyer B., Saltonstall M. BeyondCorp: Design to deployment at Google. 2016. 41(1). P. 28–34.

26. Hirning D. Implementing a Zero Trust Security Model at Microsoft. 2025. URL: https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/.

27. AWS Prescriptive Guidance: Embracing Zero Trust: A strategy for secure and agile business transformation. 2025. URL: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/strategy-zero-trust-architecture/strategy-zero-trust-architecture.pdf.

28. ON2IT. A Hands-on Approach to Zero Trust Implementation. 2020. URL: https://www.cymbel.com/wp-content/uploads/2020/10/A-hands-on-approach-to-Zero-Trust-implementation.pdf.

29. Best Practices Implementing Zero Trust with Palo Alto Networks. Palo Alto Networks, Inc. 2024. URL: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/best-practices/zero-trust-best-practices/zero-trust-best-practices.pdf.

30. Garbis J., Chapman J. W. Zero Trust Security: An Enterprise Guide. Berkeley, CA : Apress, 2021. 300 p.

31. Ross R., Winstead M., McEvilley M. Engineering Trustworthy Secure Systems // NIST Special Publication. NIST SP 800-160v1r1. 2022. 195 p. https://doi.org/10.6028/NIST.SP.800-160v1r1.

32. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof-systems // Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85). Association for Computing Machinery, New York, NY, USA, 1985. P. 291–304. https://doi.org/10.1145/22145.22178.

33. Fiege U., Fiat A., Shamir A. Zero knowledge proofs of identity // Proceedings of the nineteenth annual ACM symposium on Theory of computing. 1987. P. 210–217. https://doi.org/10.1145/28395.28419.

34. Blum M., Feldman P., Micali S. Non-interactive zero-knowledge and its applications // Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC '88). Association for Computing Machinery, New York, NY, USA, 1988. P. 103–112. https://doi.org/10.1145/62212.62222.

35. Goldreich O. Foundations of Cryptography. Basic Tools (Vol. 1). Cambridge University Press, 2001. 372 p.

36. Ben-Sasson E., Chiesa A., Tromer E., Virza, M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture // 23rd USENIX Security Symposium (USENIX Security 14). August 20-22, 2014. San Diego, CA. 2014. P. 781–796. URL: https://eprint.iacr.org/2013/879.pdf.

37. Cloud Security Alliance (CSA). Software-Defined Perimeter (SDP) Specification v2.0. (2022). URL: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2.

38. Chailloux A., Ciocan D. F., Kerenidis I., Vadhan S. (2008). Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model // Canetti R. (eds) Theory of Cryptography. TCC 2008. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2008. Vol. 4948. P. 501–534. https://doi.org/10.1007/978-3-540-78524-8_28.

39. Junkai L., Daqi H., Pengfei W., Yunbo Y., Qingni S., Zhonghai W. SoK: Understanding zk-SNARKs: The Gap Between Research and Practice. arXiv. arXiv:2502.02387. 2025. 24 p. https://doi.org/10.48550/arXiv.2502.02387.

40. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // Cryptology ePrint Archive. 2018. 046.

41. Liskov M. Updatable Zero-Knowledge Databases // Roy B. (eds) Advances in Cryptology – ASIACRYPT 2005. ASIACRYPT 2005. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2005. Vol. 3788. P. 174–198. https://doi.org/10.1007/11593447_10.

42. American Council for Technology and Industry Advisory Council (ACT-IAC). Zero Trust Cybersecurity Current Trends. 2019. 29 p. URL: https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends.

43. Department of Defense (DOD). Zero Trust Reference Architecture. Version 1.0. 2021. URL: https://www.texasre.org/Documents/Resource%20Hub/Cybersecurity/Zero%20Trust%20Reference%20Architecture.pdf.

44. Department of Defense (DoD). Zero Trust Strategy. The US Department of Defense. Version 2.0. 2022. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

45. Department of Defense (DoD). Zero Trust Reference Architecture. Version 2.0. Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team. 2022. 104 p. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

46. Badshah S., Khan A. A., Khan B. Towards process improvement in DevOps: A systematic literature review // Proceedings of the 24th International Conference on Evaluation and Assessment in Software Engineering. (EASE '20). Association for Computing Machinery, New York, NY, USA. 2020. P. 427–433. http://dx.doi.org/10.1145/3383219.3383280.

47. Davis J., Daniels R. Effective DevOps: Building a Culture of Collaboration, Affinity, and Tooling at Scale 1st Ed. O'Reilly Media, Inc. 2016. 408 p.

48. Сусукайло В. А. Використання підходу DevSecOps для аналізу сучасних загроз інформаційної безпеки // Кібербезпека: освіта, наука, техніка. 2021. 2(14). С. 26–35. https://doi.org/10.28925/2663-4023.2021.14.2635.

49. Prates L., Pereira R. DevSecOps practices and tools // International Journal of Information Security. 2024. Vol. 24. 11. https://doi.org/10.1007/s10207-024-00914-z.

50. Turner S., Holmes D., Cunningham C., Budge J., McKay P., Cser A., Shey H., Maxim M. A. A Practical Guide To A Zero Trust Implementation. Forrester Research, Inc. 2021. 14 p. URL: https://www.forrester.com/report/a-practical-guide-to-a-zero-trust-implementation/RES157736.

51. Uttecht K. D. Zero trust (ZT) concepts for federal government architectures // MIT Lincoln Laboratory. 2020. 58 p. URL: https://apps.dtic.mil/sti/pdfs/AD1108910.pdf.

52. Peck J., Beyer B., Beske C., Saltonstall M. Migrating to BeyondCorp // Maintaining productivity while improving security. 2017. 42(2). P. 1–7.
URL: https://www.usenix.org/system/files/login/articles/login_summer17_10_peck.pdf.

53. Chandramouli R., Butcher Z. NIST Special Publication 800-207A. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments // National Institute of Standards and Technology. 2023. 31 p. https://doi.org/10.6028/NIST.SP.800-207A.

54. Collier Z. A., Sarkis J. The zero trust supply chain: Managing supply chain risk in the absence of trust // International Journal of Production Research. 2021. 59(11). P. 3430–3445.
https://doi.org/10.1080/00207543.2021.1884311.

55. Sin L.W., Samsudin A.E., Zengeni I.P., Zolkipli M.F. Zero Trust Security Models in Penetration Testing // International Journal of Advances in Engineering and Management (IJAEM). 2024. 6(7). P. 442–450. URL: https://ijaem.net/issue_dcp/Zero%20Trust%20Security%20Models%20in%20Penetration%20Testing.pdf.

56. Akamai Security. A Blueprint for Building a Zero Trust Architecture. 2024. URL: https://www.akamai.com/site/en/documents/white-paper/a-blueprint-for-building-a-zero-trust-architecture-white-paper.pdf.

57. Adahman Z., Malik A.W., Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security // Computers & Security. 2022. 122(1). 102911. https://doi.org/10.1016/j.cose.2022.102911.

58. Mavroudis V. Zero-Trust Network Access (ZTNA). arXiv. 2024. 10 p. https://doi.org/10.48550/arXiv.2410.20611.

59. Al-Ofeishat H., Alshorman R. Build a Secure Network Using Segmentation and Micro-segmentation Techniques // International Journal of Computing and Digital Systems. 2024. 16(1). P. 1499–1508. http://dx.doi.org/10.12785/ijcds/1601111.

60. Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy. 2021. URL: https://www.pwc.com/sg/en/publications/assets/page/zero-trust-architecture.pdf.

61. Ahmed I., Nahar T., Urmi S. S., Taher K. A. Protection of Sensitive Data in Zero Trust Model. In Proceedings of the International Conference on Computing Advancements (ICCA '20) // Association for Computing Machinery, New York, NY, USA. 2020. 63(1). P. 1–5. https://doi.org/10.1145/3377049.3377114.

62. Microsoft. Zero Trust deployment plan with Microsoft 365. 2025. URL: https://learn.microsoft.com/en-us/microsoft-365/security/microsoft-365-zero-trust.

63. Kinyua J., Awuah L. AI/ML in security orchestration, automation and response: Future research directions // Intelligent Automation & Soft Computing. 2021. 28(2). P. 527–545. https://doi.org/10.32604/iasc.2021.016240.

64. He Y., Huang D., Chen L., Ni Y., Ma X. A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing. 2022. 13 p. https://doi.org/10.1155/2022/6476274.

Надійшла до редколегії 07.06.2025

Відомості про авторів:

Єсін Віталій Іванович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-наукового інституту комп'ютерних наук та штучного інтелекту; Україна; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

Бородавка Владислав Вячеславович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-наукового інституту комп'ютерних наук та штучного інтелекту; Україна; e-mail: vladyslav.borodavka@karazin.ua; ORCID: https://orcid.org/0009-0002-3885-1364