УДК 004.05 **DOI:10.30837/rt.2024.2.217.03**

В.І. ЄСІН, д-р техн. наук, В.В. ВІЛІГУРА, Д.Ю. УЗЛОВ, канд. техн. наук

ОГЛЯД ІСНУЮЧИХ МОДЕЛЕЙ ТА ОСНОВНИХ ПРИНЦИПІВ НУЛЬОВОЇ ДОВІРИ

Вступ

Виклики безпеки XXI століття характеризуються змінами та непередбачуваністю [1]. Диджиталізація (digitalization) нашого світу веде до зростання кількості комунікацій. Останні тенденції, такі як хмарні обчислення, Інтернет речей та використання концепцій CYOD та BYOD призводять до збільшення розмірів існуючих мереж. Все більше і більше пристроїв та сервісів обмінюються інформацією всередині корпоративних мереж, а також за їх межами. Ці зміни призводять до появи нових складних вимог до мережевої безпеки, яким існуючі рішення слабо відповідають [2], про що свідчить зростання кількості витоків даних та хакерських атак (зломи стають все масштабнішими та сміливішими, зачіпаючи все: від баз даних клієнтів та громадян до даних про вакцини та маршрутизатори Wi-Fi [3]). Як відомо, традиційна мережева безпека фокусується на захисті периметра. Тобто більшість концепцій мережевої безпеки ґрунтуються на розподілі внутрішніх та зовнішніх мереж. Всі користувачі, пристрої та служби у захищеній внутрішній мережі вважаються довіреними, тоді як зовнішні користувачі, пристрої та служби класифікуються як ненадійні. Однак недоліки цього підходу стають очевидними, якщо врахувати, що зловмисники у разі компрометації суб'єктів (кінцевих користувачів, застосунків та інших нефізичних сутностей), які запитують інформацію та часто отримують широкий доступ до безлічі корпоративних ресурсів, шляхом видачі себе за іншу особу та ескалації (підвищення привілеїв) можуть отримати доступ до ресурсів усередині або за межами мережі. Більше того, багато підприємств (організацій, компаній) не мають чітко визначеного периметра. Периметр втрачає свою актуальність через кілька факторів, включаючи зростання хмарних обчислень, мобільність та зміни у сучасному штаті співробітників (використання віддалених працівників) [4]. Крім того, загрозу становлять і внутрішні зловмисники (інсайдери). Таким чином, ідея про те, що жодна мережа (ні внутрішня, ні зовнішня) не заслуговує на довіру, набирає обертів як у наукових колах, так і на практиці [2].

Щоб захистити сучасне цифрове підприємство, необхідна комплексна стратегія для безпечного доступу у будь-який час і в будь-якому місці до своїх корпоративних ресурсів (застосунків, застарілих/успадкованих систем, даних, пристроїв тощо) незалежно від того, де вони розташовані [5]. Дійсно, зростання хмарних обчислень, Інтернету речей, бізнес-партнерів та зростаючої кількості віддалених працівників підвищує складність захисту цифрових ресурсів підприємства, оскільки існує більше точок входу, виходу та доступу до даних, ніж будь-коли раніше, а існуючі рішення відчувають труднощі з реагуванням на динамічні зміни, оскільки вони часто складаються зі статичних наборів правил, міжмережевих екранів, VPN та підмереж. Внутрішня мережа захищена настільки, наскільки захищено найгірше захищений пристрій або застосунок. Заходів, що обмежують бічне переміщення (lateral movement) по мережі, або дуже мало, або вони взагалі відсутні. IP-адреси пристроїв та сервісів відомі ззовні. Існуючі рішення спочатку встановлюють з'єднання, а потім перевіряють права доступу. Це робить їх потенційними цілями, які можна використовувати для проникнення в мережу або порушення її роботи, наприклад, за допомогою розподілених атак типу «відмова в обслуговуванні» (DDoS). Файли журналів зберігаються на централізованих серверах журналів. Отримавши доступ до таких файлів, зловмисники можуть замаскувати свою діяльність та стерти сліди [2]. Тому підприємства сьогодні переосмислюють традиційний периметр безпеки мережі, схиляючись до нової концепції та архітектури захисту.

Такою концепцією стала сьогодні парадигма безпеки, що отримала назву «нульова довіра» (Zero Trust – ZT). За своєю суттю «нульова довіра» – це філософія, підхід та набір керівних принципів кібербезпеки, що використовуються для створення стратегії, яка фокусується

на переміщенні захисту мережі від широких статичних периметрів мережі до вужчого зосередження уваги на суб'єктах, активах підприємства (а саме, пристроях, компонентах інфраструктури, застосунках, віртуальних та хмарних компонентах) та окремих або невеликих групах ресурсів [4, 6, 7]. Нульова довіра – це не єдина архітектура, а набір керівних принципів для робочого процесу, проєктування системи та операцій, які можна використовувати для покращення стану безпеки будь-якої класифікації або рівня чутливості [7]. Основна ідея концепції нульової довіри полягає в тому, що не існує областей, які заслуговують на довіру. І її основний принцип «ніколи не довіряти, завжди перевіряти» [8]. Цей більш обмежувальний підхід спрямовано на поліпшення захисту ресурсів. Хоча «нульова довіра» починалася як вузькоспрямований підхід, який полягає в тому, щоб не довіряти жодним мережевим ідентифікаційним/обліковим даним (ідентифікаторам) доти, доки вони не будуть автентифіковані та авторизовані, його масштаби по праву розширилися, щоб забезпечити набагато ширший набір можливостей безпеки у середовищі підприємства (організації, компанії, корпорації). Архітектура нульової довіри (zero trust architecture – ZTA) враховує нові тенденції, приділяючи особливу увагу захисту ресурсів, а не периметру мережі, оскільки розташування мережі більше не розглядається як основний компонент забезпечення безпеки, необхідної для ресурсу [4, 7]. ZTA ніколи не надає доступ до ресурсів до тих пір, поки суб'єкт, актив (це елемент/об'єкт, що представляє цінність для зацікавлених сторін); актив може бути матеріальним (наприклад, фізичний об'єкт, такий як апаратне забезпечення, вбудоване програмне забезпечення, обчислювальна платформа, мережевий пристрій або інший технологічний компонент) або нематеріальним (наприклад, люди, дані, інформація, програмне забезпечення, можливості, функції, послуги, товарний знак, авторське право, патент, інтелектуальна власність, імідж чи репутація) [9]) або робоче навантаження не будуть верифіковані за допомогою процедур автентифікації та прав/дозволів на виконання певних дій (авторизації) [4].

Згідно з результатами дослідження, проведеного компанією Grand View Research, обсяг світового ринку систем безпеки з нульовою довірою в 2022 р. склав 24,84 мільярда доларів США, а в період з 2023 по 2030 р. очікується сукупний середньорічний темп зростання (CAGR – compound annual growth rate) на рівні 16,6 % (що за прогнозами дозволить вийти на цифру 82,45 мільярда доларів США до 2030 р.) [10, 11]. Gartner, Inc. прогнозує, що до 2026 р. 10 % великих підприємств матимуть зрілу та вимірну програму нульової довіри порівняно з менш ніж 1 % у 2023 р. [12].

Однак, незважаючи на популяризацію концепції нульової довіри та очевидні переваги у сфері безпеки від її застосування, на підприємствах виникають певні складнощі щодо її реалізації [13 – 15]. Якщо у 2021 р. згідно зі звітом компанії Fortinet [13], 40 % респондентів заявили, що їхня стратегія нульової довіри повністю реалізована, то у 2023 р. лише 28 % компаній оголосили про те, що вони вже мають повне рішення з нульовою довірою. Ці цифри показують, що, швидше за все, робота з впровадження концепції нульової довіри виявилася трохи складнішою, ніж передбачалося. Деякі проблеми стали очевидними лише після того, як кілька рішень вже були впроваджені, і виникла потреба у взаємодії між розрізненими рішеннями. Основними серйозними факторами, що перешкоджають, за даними того ж звіту, стали брак інформації для вибору рішення з нульовою довірою (на нього вказали 16 % організацій, у тому числі 24 % серед невеликих компаній) та відсутність кваліфікованих розробників/постачальників (на нього вказали 24 % організацій). 4 % організацій з опитаних вказали на нестачу людських ресурсів. Ще одним важливим висновком цього звіту є те, що розгортання рішень від кількох постачальників створює нові проблеми для організацій, включаючи ненавмисне створення проблем з безпекою та високі операційні витрати через розростання постачальників і рішень (на відсутність необхідних бюджетних коштів для проведення IT-змін прямо зараз – вказали 17 % організацій).

Як видно з викладеного, існує проблема, пов'язана з певним дефіцитом поінформованості про підхід нульової довіри (про його теоретичний та практичний потенціал) для вибору правильного рішення. Стаття націлена на вирішення цієї проблеми шляхом узагальнення

наявних досліджень та досвіду різних міжнародних компаній, які впроваджують даний підхід на практиці. У стислому викладі розглядаються моделі та ключові принципи нульової довіри, запропоновані відомими міжнародними організаціями та компаніями, які допоможуть розібратися у фундаментальному зрушенні у підході до інформаційної безпеки, кібербезпеки. Дослідження, що проводились у цій роботі, спираються на публікації різних міжнародних авторитетних видань (у тому числі стандартів та деяких урядових організацій по всьому світу), присвячених концепції нульової довіри.

1. Історія та еволюція концепції нульової довіри

Концепція нульової довіри стала відомою в кібербезпеці ще до появи терміну «нульова довіра», який був представлений у звіті [16] відомої американської дослідницької та консалтингової компанії Forrester (одного з ключових дослідників ринків інформаційних технологій). Ідея концепції, згідно з якою жодному учаснику мережі (як внутрішньої, так і зовнішньої) не можна довіряти, а будь-який доступ до ресурсів підприємства є потенційною загрозою, виникла ще на початку розвитку безпечних обчислень [2]. Так, ще 1975 р. автори роботи [17] пропонували повне посередництво у доступі та мінімальні привілеї. У 2007 р. Агентство оборонних інформаційних систем (DISA – Defense Information Systems Agency) та Міністерство оборони (Department of Defense – DoD) США опублікували свою роботу щодо більш безпечної корпоративної стратегії під назвою «чорне ядро» («black core») [1]. Чорне ядро передбачало перехід від моделі безпеки на основі периметра до такої, яка зосереджена на безпеці окремих транзакцій. В результаті роботи Jericho Forum міжнародною групою в галузі безпеки було оприлюднено ідею деперіметризації (de-perimeterization) [18] – обмеження неявної довіри на основі розташування мережі та обмеження покладатися на єдиний статичний захист у великому сегменті мережі [7]. Далі концепції деперіметризації розвивалися і вдосконалювалися, перетворюючись на ширшу концепцію, а саме концепцію нульової довіри. У звіті Forrester [16] відображено ідеї, які обговорювалися в галузі протягом кількох років, зокрема, при нульовій довірі весь мережевий трафік не є довіреним. Тобто фахівці з безпеки повинні: перевіряти та захищати всі ресурси; обмежувати та суворо забезпечувати контроль доступу; перевіряти та реєструвати весь мережевий трафік. Згодом у компанії Forrester розвинули концепцію нульової довіри, у ту, що зараз відома, як *розширення «нульової довіри»* (Zero Trust eXtended – ZTX) [19].

Приблизно в той же час Google розпочала свою реалізацію концепції комп'ютерної безпеки з нульовою довірою (BeyondCorp), яка переносить контроль доступу з традиційного периметру мережі на окремі пристрої та користувачів. Серія статей, починаючи з 2014 р., компанії Google [20 – 26] сприяли внесенню значного внеску до концепції комп'ютерної безпеки з нульовою довірою. BeyondCorp використовує низку політик безпеки, включаючи автентифікацію, авторизацію та контроль доступу, щоб гарантувати, що лише авторизовані користувачі можуть отримати доступ до корпоративних ресурсів. BeyondCorp складається з безлічі взаємодіючих компонентів, які гарантують, що лише пристрої та користувачі, що пройшли відповідну автентифікацію, мають право доступу до необхідних корпоративних застосунків [20].

У 2017 р. провідна світова дослідницька та консалтингова компанія у сфері інформаційних технологій Gartner, Inc. переглянула та оновила свою концепцію *безперервної адаптивної оцінки ризиків та довіри* (*Continuous Adaptive Risk and Trust Assessment* – CARTA), яка має багато загальних принципів із нульовою довірою. CARTA [27] надає не тільки елементи ідентифікації та даних, але також включає ризики та положення, пов'язані з ідентифікацією та пристроями, що мають доступ до середовища.

Завдяки публікації Національного інституту стандартів та технологій США (NIST) про архітектуру нульової довіри [7], а також пов'язаної з нею проєктом Національного центру передового досвіду в галузі кібербезпеки США (US National Cybersecurity Center of Excellence – NCCoE) [4], концепції нульової довіри у масштабах корпоративної мережевої безпеки

та безпеки даних підприємств стали приділяти більшої уваги. Федеральним агентствам вже понад десять років рекомендується перейти до безпеки, заснованої на принципах нульової довіри, створюючи можливості та політики, такі як Федеральний закон про модернізацію інформаційної безпеки (*Federal Information Security Modernization Act* – FISMA), якому підпорядковуються Система управління ризиками (*Risk Management Framework* – RMF); Федеральне управління ідентифікацією, обліковими даними та доступом (*Federal Identity, Credential, and Access Management* – FICAM); Довірені підключення до Інтернету (*Trusted Internet Connections* – TIC); і програми/системи безперервної діагностики та пом'якшення наслідків (*Continuous Diagnostics and Mitigation* – CDM). Усі ці програми спрямовані на обмеження доступу до даних і ресурсів для авторизованих сторін. Коли ці програми починалися, вони були обмежені технічними можливостями інформаційних систем. Політики безпеки були здебільшого статичними та застосовувалися у вузлових точках, які підприємство могло контролювати, щоб отримати найбільший ефект від вкладених зусиль. У міру розвитку технологій з'явилася можливість для безперервного детального аналізу та оцінки запитів на надання доступу (відповідно до принципу необхідності доступу), щоб знизити ризик втрати даних через злому облікових записів, атак зловмисників, що стежать за мережею та інших загроз [7]. І тепер уже відповідно до концепції нульової довіри забезпечується детальний контроль доступу з урахуванням ідентифікаційних та контекстно-залежних даних, що реалізується автоматично спеціалізованою системою.

Окремі принципи нульової довіри самі по собі не нові, новим є той факт, що всі ці принципи використовуються комплексно для захисту ресурсів підприємства [2]. При традиційному управлінні доступом права (привілеї) зазвичай призначаються заздалегідь з урахуванням посади (виконуваних функціональних обов'язків), а в рішеннях з нульовою довірою з'являється додатковий механізм – центр (пункт, точка) прийняття рішення про політику, що забезпечує динамічне прийняття рішень про доступ на основі наявних політик, а також вхідних даних із деяких важливих зовнішніх джерел. Якщо традиційні системи управління доступом розроблялися в основному з орієнтацією на користувача, то в епоху цифрової трансформації контроль доступу повинен також поширюватися на автономні системи та інтелектуальні агенти, що й робиться в рішеннях, створюваних на основі концепції нульової довіри. Слід зауважити, що, хоча автоматичні дії є основними в операційній діяльності в нових умовах, це не скасовує можливості використання у нових системах ручного втручання або включення в робочий процес конкретних дій вручну перед активацією автоматичного реагування. Крім того, сьогодні є деякі недостатньо ефективні (або вже застарілі) рішення (приклади деяких з них наведені в табл. 1), які вимагають заміни або модифікації, вдосконалення, адаптації до вимог систем, відповідним стратегії нульової довіри.

Таблиця 1

Існуючі рішення безпеки та їх недоліки

Існуючі рішення	**Недоліки рішення**
Перепустки	Втрата носія або його викрадення.
Сегментація за допомогою DNS-сервера	Занадто широкий доступ до мережі.
NAC (*Network Access Control*)	Коштовність та недостатня швидкість, відсутність можливості використання для хмарних середовищ.
IDS/IPS (*Intrusion Detection System / Intrusion Prevention System*)	Відсутність можливості застосування у хмарному середовищі, наявні помилкові спрацьовування при перевірці доступу.
VPN	Занадто проста процедура отримання доступу, надає широкий доступ до мережі.
SIEM (*Security Information* and *Event Management*)	Відсутність можливості керування віддаленим доступом.

Якщо порівнювати традиційну модель безпеки (безпеки периметра) і модель нульової довіри, то слід звернути на їхню принципову відмінність – модель нульової довіри не має

«зони довіри» і заснована на перевірці без довіри, навіть якщо це внутрішній користувач. У той час як модель безпеки периметра орієнтована на блокування, модель нульової довіри передбачає ретельну та постійну перевірку кожного користувача та пристрою, що намагається підключитися до ресурсів, незалежно від їхнього розташування [28]. Ці та інші аспекти характерних відмінностей даних моделей наведені в табл. 2.

Таблиця 2

Порівняння традиційної моделі безпеки та моделі нульової довіри

Характеристика	**Традиційна модель безпеки**	**Модель нульової довіри**
Підхід	Довіряй але перевіряй.	Нікому не довіряй і все перевіряй.
Межа довіри	Зовнішня (немає довіри – non trust). Внутрішня (довірена – trust).	Мікросегментація (мережі поділяються на дрібніші сегменти або безпечні зони, щоб обмежити бічне переміщення (lateral movement) загроз; кожен сегмент має свої засоби керування доступом користувачів та політики безпеки).
Мережева архітектура	Модель «замок та рів» (castle and moat) з підвищеним акцентом на захист периметра.	Децентралізована та мікросегментована, з детальним контролем доступу.
Контроль доступу	Контроль доступу на основі IP.	Керування доступом, орієнтоване на дані.
Автентифікація	Після перевірки при початковому доступі.	Перед доступом та постійна перевірка.
Керування безпекою	Індивідуальний моніторинг та видимість.	Видимість, автоматизація та оркестрування поведінки, пристроїв, сервісів/послуг та безпеки.
Політика безпеки	Заздалегідь встановлені правила та загальна політика.	Деталізовані правила та адаптивні політики (оцінка рівня безпеки).
Шифрування зв'язку	Зовнішня мережа (шифрування). Внутрішня (без шифрування).	Повне шифрування трафіку.
Реагування на порушення	Як тільки периметр порушено, зловмисники можуть здобути свободу дій.	Навіть якщо порушення сталося, переміщення зловмисників ретельно відстежуються.

В цілому ж, архітектура нульової довіри – це комплексний/наскрізний (end-to-end) підхід до корпоративних ресурсів і безпеки даних, який охоплює ідентифікацію фізичних та нефізичних осіб/сутностей, облікові дані, керування доступом, операції, кінцеві точки, середовища розміщення та інфраструктуру взаємозв’язку [7]. Інтеграція раніше розрізнених засобів забезпечення безпеки, систем інфраструктури та корпоративних систем має важливе значення. Інтеграція засобів ідентифікації та безпеки дозволяє створити комплексний механізм безпеки, за допомогою якого рішення нульової довіри можуть забезпечити безпечніше середовище.

При цьому слід зазначити, що концепція нульової довіри продовжує розвиватися в міру того, як постачальники та організації зі стандартизації переглядають та вдосконалюють специфікації та реалізації нульової довіри, визнаючи це фундаментальною зміною у підході до інформаційної безпеки [6].

2. Моделі нульової довіри

2.1. Розширена модель нульової довіри компанії Forrester

Компанія Forrester, як зазначалося вище, випустила свою першу модель нульової довіри у 2010 р., яку у наступні роки переглянула та внесла зміни. В результаті було створено так звану розширену модель нульової довіри (ZTX – Zero Trust eXtended) [19], в якій було виділено сім компонентів нульової довіри: п'ять для контролю безпеки та два – для взаємодії між компонентами (рис. 1). Розглянемо їх докладніше.

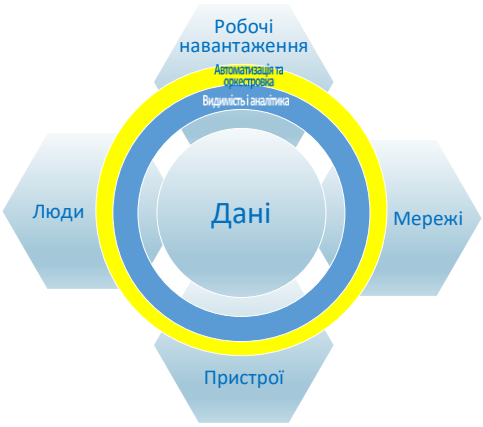

Рис. 1. Розширена модель нульової довіри компанії Forrester

Розширена модель нульової довіри надає багатший контент і всебічну модель, в якій дані розташовуються в центрі (рис. 1). При цьому фахівці Forrester загострюють увагу на тому, що різке збільшення обсягу даних як у локальних, так і в хмарних середовищах загострює проблему їх захисту, яку необхідно вирішувати та вирішувати її треба, виходячи з нових вимог та можливостей нових технологій та підходів.

Отже, *дані* (*data*) є центром моделі ZTX (рис. 1), а безпека даних є одним із стовпів стратегії нульової довіри. Захист даних та керування ними, категоризація та розробка схем класифікації даних, а також шифрування даних як при зберіганні, так і при передачі є ключовими елементами будь-якого підходу з нульовою довірою. Крім того, повинна бути система запобігання втраті даних (*Data Loss Prevention* – DLP), яка повинна бути частиною архітектури нульової довіри, а також бути пов'язаною з моделлю політики з можливістю застосування політик контекстного доступу, де тільки це можливо.

Оточуючі елементи – *робочі навантаження* (*workloads*), *мережі* (*networks*), *пристрої* (*devices*) і *люди* (*people*) – є провідниками даних і, отже, також потребують захисту.

Мережевий компонент (стовп) моделі ZTX в першу чергу орієнтований на сегментацію мережі (як на рівні користувачів, так і на рівні сервера) для забезпечення кращої безпеки на основі атрибутів, пов'язаних з ідентифікаційними даними. Здатність сегментувати, ізолювати та контролювати мережу є ключовим елементом управління для нульової довіри. При цьому слід розуміти, що підприємства сьогодні мають багато різних компонентів, що становлять традиційну інфраструктуру мережевої безпеки. Це і міжмережеві екрани наступного покоління (Next-Generation Firewalls – NGFW), і міжмережові екрани веб-застосунків (Web Application Firewalls – WAF), і рішення для контролю доступу до мережі (NAC), і системи захисту від вторгнень (Intrusion Protection Systems – IPS). Як правило, всі ці компоненти відіграють важливу роль і в рамках концепції нульової довіри.

Компонент (стовп) моделі ZTX «*Люди*». Останнім рубежем будь-якої стратегії нульової довіри є встановлення та суворе дотримання обмежень на доступ користувачів, а також забезпечення їхньої безпеки при взаємодії з Інтернет-ресурсами. З позиції Forrester, даний компонент повинен включати кілька елементів системи керування ідентифікацією і доступом (Identity and Access Management – IAM), в рамках якої відмінно себе зарекомендували такі добре вивчені моделі, як управління доступом на основі ролей (Role-Based Access Control – RBAC) та атрибутів (Attribute-Based Access Control – ABAC). При цьому технологія нульової довіри дозволяє використовувати дані моделі більш широко та ефективно у всій корпоративній інфраструктурі. Важливе значення для реалізації технології нульової довіри, як ключових елементів у рамках компонента «*Люди*», також мають багатофакторна автентифікація (Multi-Factor Authentication – MFA) та система єдиного входу (Single Sign On – SSO) з використанням сучасних відкритих стандартів, таких як OAuth та SAML.

Робочі навантаження – це термін високого рівня, який за визначенням Forrester, відноситься до всього стеку застосунків, від рівня застосунку до гіпервізора або автономних

компонентів обробки, таких як контейнери і віртуальні машини [19]. Ці застосунки слід розглядати як вектор загрози (особливе занепокоєння викликають робочі навантаження, що виконуються в публічних хмарах), і до них мають бути застосовані елементи керування та технології нульової довіри. Для нульової довіри потрібне управління доступом до робочого навантаження на основі метаданих, що послідовно застосовується в гібридних середовищах.

Пристрої з нульовою довірою. Технології Інтернету речей та мережевих пристроїв створили величезну сферу потенційного ризику для мереж та підприємств. Розумні (smart), мобільні пристрої сьогодні набули широкого поширення по всьому ринку товарів. Однак у результаті такого прориву виявився зворотний бік цього процесу – відкрилися нові можливості шляхів поширення коду та засобів, які фахівці безпеки повинні відстежувати та розглядати як ненадійні у будь-якій інфраструктурі. Щоб дійсно перейти до стратегії нульової довіри, фахівці з безпеки повинні мати можливість постійно ізолювати, захищати і контролювати кожен пристрій у мережі [19]. Іншими словами, модель безпеки для *Пристроїв* повинна включати ідентифікацію, облік, ізоляцію, безпеку та контроль пристрою.

Видимість та аналітика/аналіз (*Visibility and Analytics*). Не можна боротися з загрозою, яка невидима і яку ви не розумієте. Тому сьогодні пропонуються такі інструменти, як традиційне керування інформацією про безпеку (*security information management* – SIM – це популярний вираз, що означає метод збору, організації та складання звітів із записів, пов'язаних з інформаційною безпекою [29]), а також більш просунуті платформи аналізу безпеки, системи аналізу поведінки користувачів з погляду безпеки (*security user behavior analytics – SuBa*) та інші аналітичні системи, які дозволяють фахівцям з безпеки знати та розуміти, що відбувається у мережі. Ці інструменти, платформи, системи допомагають аналітику з безпеки ретельно стежити за існуючими загрозами та грамотніше організовувати захист. Хоча сьогодні немає жодної платформи, яка охоплювала б необхідну широту функціональності. Але ця область сьогодні активно розвивається [6]. Таким чином, *видимість та аналітика/аналіз* усередині ZTX – це використання та подання даних по всьому підприємству для підтримки обґрунтованих рішень щодо безпеки на основі контекстної інформації.

Автоматизація (*automation*) та *оркестрування/оркестрація* (*orchestration*) у ZTX необхідні для автоматизації ручних процесів та їх зв'язку з політикою безпеки та діями з реагування. *Оркестрування* – це: а) автоматизоване конфігурування/налаштування, координація та керування комп'ютерними системами та програмним забезпеченням [30]; б) шаблон взаємодії, якому повинен слідувати агент веб-служби для досягнення своєї мети; *оркестрування* визначає послідовність та умови, в яких одна веб-служба викликає інші веб-служби для реалізації деякої корисної функції [31]). Вважається, що елемент автоматизації та оркестрування має вирішальне значення для успіху парадигми нульової довіри. Нульова довіра за своєю суттю є динамічною та адаптивною, і єдиний спосіб досягти цього – це автоматизувати та оркеструвати все корпоративне середовище. Можливість мати ефективне керування та контроль над багатьма компонентами, що використовуються в рамках стратегії нульової довіри, є життєво важливою частиною ZTX.

Сьогодні Агентство з кібербезпеки та безпеки інфраструктури (CISA – Cybersecurity and Infrastructure Security Agency), а також Адміністративно-бюджетне управління США (OMB – US Office of Management and Budget – Офіс менеджменту та бюджету США) визнають ці сім компонентів і додають ще один: керівництво (governance) [32]. На рис. 2 наведено зіставлення компонентів ZTX Forrester із стовпами CISA для сучасної нульової довіри.

На рис. 2 (праворуч) показані такі компоненти (стовпи CISA), як *ідентичність*, *пристрої, мережі*, *програми* (*застосунки*) та *робочі навантаження*, а також *дані*. Компоненти «*Видимість та аналітика/аналіз*», «*Автоматизація та оркестрування*» та «*Керівництво*» надають можливості для інтеграції передових досягнень по кожному з наведених вище п'яти компонентів. Розглянемо їх докладніше (у тому числі, уточнюючи раніше дані деяким з них визначення та характеристики).

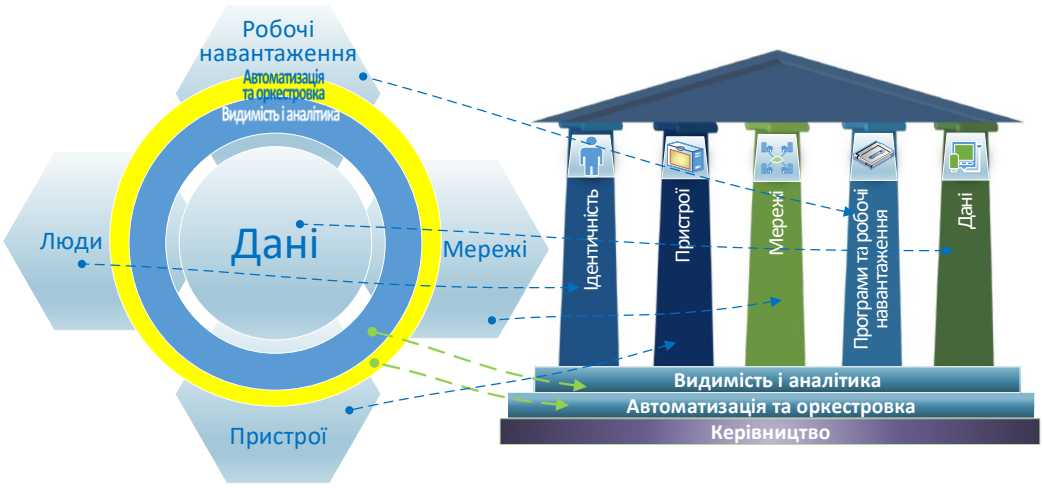

Рис. 2. Зіставлення розширеної моделі нульової довіри Forrester зі стовпами CISA

Ідентичність (*identity*) – це: а) атрибут або набір атрибутів, які однозначно описують користувача або сутність (суб'єкт; під сутностями розуміються користувачі, служби, дані, комп'ютери тощо [33]) підприємства/організації, включаючи сутності, що не є фізичними особами [27]; б) набір значень атрибутів (характеристик), за якими можна розпізнати сутність та які в рамках відповідальності/повноважень спеціаліста з управління ідентифікацією достатні для того, щоб відрізнити цю сутність від будь-якої іншої [34]; в) атрибут або набір атрибутів, які однозначно описують суб'єкт у даному контексті [35, 36].

Говорячи про ідентичність, слід зазначити, що підприємства (організації, компанії, установи) повинні гарантувати та забезпечувати доступ користувачів та суб'єктів до необхідних ресурсів у потрібний час та для певних цілей, не надаючи надмірного доступу. Крім того, вони повинні інтегрувати рішення з керування ідентифікацією, обліковими даними та доступом, за можливістю в рамках всього підприємства, щоб забезпечити сувору автентифікацію, надавати індивідуальну авторизацію (дозволи, повноваження, права) на основі контексту та оцінювати ризики ідентифікації для користувачів та сутностей / суб'єктів цього підприємства. При необхідності організаціям слід інтегрувати свої системи зберігання та управління ідентифікаційними даними, щоб підвищити обізнаність про ідентифікаційні дані підприємства та пов'язані з ними обов'язки та повноваження [32].

Пристрої. Під пристроєм розуміється будь-який актив (включаючи його апаратне та програмне забезпечення, вбудоване мікропрограмне забезпечення (firmware) тощо), який може підключатися до мережі, у тому числі сервери, настільні комп'ютери (desktop) та ноутбуки (laptop), принтери, мобільні телефони, пристрої IoT (internet of things), мережеве обладнання та багато іншого. Пристрої можуть належати установі або бути власністю співробітників (BYOD – bring-your-own-device), партнерів чи відвідувачів. Підприємства повинні забезпечувати безпеку всіх пристроїв підприємства, керувати ризиками авторизованих пристроїв, які не контролюються підприємством, та запобігати доступу неавторизованих пристроїв до ресурсів. Керування пристроями включає ведення динамічної реєстрації всіх активів, включаючи їх апаратне і програмне забезпечення, вбудоване мікропрограмне забезпечення і т. д., а також їх конфігурацій і пов'язаних з ними вразливостей в міру їх виявлення.

Мережі. Під мережею розуміється відкрите комунікаційне середовище, що включає такі типові канали, як внутрішні мережі підприємства (організації, компанії, установи), бездротові мережі та Інтернет, а також інші потенційні канали, такі як стільниковий зв'язок та канали рівня застосунків, що використовуються для передачі повідомлень.

Програми та *робочі навантаження*. Програми (застосунки) та робочі навантаження включають корпоративні системи, комп'ютерні програми та сервіси, які виконуються в локальному середовищі (локально – on-premises), на мобільних пристроях і в хмарних середовищах.

Дані. Дані включають усі структуровані та неструктуровані файли та фрагменти, які знаходяться або знаходились у корпоративних системах, пристроях, мережах, застосунках, базах даних, об'єктах інфраструктури та резервних копіях (включаючи локальні та віртуальні середовища), а також пов'язані з ними метадані.

Компонент «*Видимість та аналітика/аналіз*» забезпечують всебічну видимість, яка є основою для прийняття стратегічних рішень та полегшує дії у відповідь (дії з реагування). Компонент «*Автоматизація та оркестровка*» використовують цю інформацію для підтримки надійних та оптимізованих операцій з обробки інцидентів безпеки та реагування на події у міру їх виникнення. Компонент «*Керівництво*» дозволяє організаціям приймати рішення на основі ризиків. Функції «*Керівництва*» пов'язані із забезпеченням організацій відповідними фахівцями, необхідними технологіями для виконання поставлених завдань з урахуванням дотримання встановлених вимог та наявних ризиків.

Важливо відзначити, що точка зору CISA спирається на початкову концепцію нульової довіри, запропоновану компанією Forrester [37].

2.2. Модель безперервної адаптивної оцінки ризиків та довіри Gartner

Gartner, Inc. підійшла до нульової довіри через свою модель безперервної адаптивної оцінки ризиків та довіри (CARTA). Метою CARTA є забезпечення безперервної оцінки ризиків, що стосуються користувачів, пристроїв, застосунків, даних та робочих навантажень з точки зору прогнозування (predict), запобігання (prevent), виявлення (detect) та реагування (respond). CARTA була представлена компанією Gartner як розвиток адаптивної архітектури безпеки (рис. 3) [38].

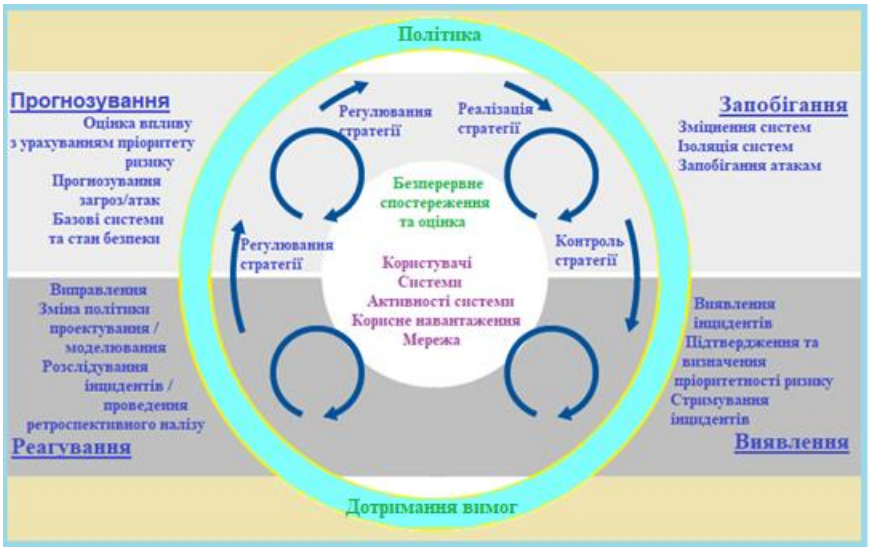

Рис. 3. Чотири складові адаптивної архітектури безпеки

CARTA використовує фундаментальний процес впровадження стратегії безпеки, моніторингу стану/положення (posture) та регулювання/коригування стратегії забезпечення безпеки через різні рівні/площини (planes) безпеки. Gartner вважає, що ці принципи повинні застосовуватися в масштабах всього підприємства і включати вимоги безпеки, політики та відповідності нормативним вимогам.

Gartner прагне розглядати нульову довіру більш вузько, використовуючи терміни доступу до мережі з нульовою довірою (Zero Trust Network Access – ZTNA) для забезпечення безпеки між користувачем та сервером та сегментація мережі з нульовою довірою (Zero Trust Network Segmentation – ZTNS) для мікросегментації / міжсерверної безпеки [6].

3. Основні принципи нульової довіри, запропоновані відомими міжнародними організаціями та компаніями

Три основні принципи – три фундаментальні концепції нульової довіри, представлені в роботі [16], опублікованій компанією Forrester, формулюються таким чином:

1. *Забезпечте безпечний доступ до всіх ресурсів, незалежно від їхнього розташування*.

Це ємне, стисло твердження, яке охоплює безліч аспектів, і в першу чергу необхідність включення всіх ресурсів у сферу компетенції рішення з нульовою довірою. Цей принцип вимагає, щоб рішення з нульовою довірою забезпечувало безпечний доступ усіх облікових записів (людини та комп'ютера) до всіх ресурсів (даних, застосунків, серверів) незалежно від місцезнаходження ідентифікатора (облікового запису сутності) та незалежно від місцезнаходження або використовуваної технології ресурсу, до якого здійснюється доступ виходячи з припущення, що весь трафік є трафіком загрози (принаймні доти, доки немає повної впевненості, що трафік авторизований, перевірений і захищений). У реальних ситуаціях це часто вимагає використання зашифрованих каналів для доступу до даних як у внутрішніх, так і в зовнішніх мережах. Що стосується другої частини принципу – «незалежно від розташування», це стає особливо актуальним в умовах переходу до хмарних технологій, коли більшість даних знаходиться поза традиційними центрами обробки даних. У цьому випадку рішення з нульовою довірою допоможе забезпечити дотримання питань, пов'язаних із розміщенням даних, відповідно до нових правил конфіденційності даних, що з'являються у всьому світі. Саме цей принцип, по суті, вимагає ліквідації традиційного корпоративного периметра та заміни його альтернативною парадигмою безпеки.

2. *Використовуйте стратегію найменших/мінімальних привілеїв та суворо дотримуйтесь принципів контролю доступу*.

Стратегія найменших привілеїв при доступі до ресурсів не є чимось новим, але до появи концепції нульової довіри її важко було реалізувати в широких масштабах. Історично склалося так, що рішення в галузі інформаційної безпеки не могли усунути розрив між забезпеченням безпеки на рівні мережі та застосунків. Сьогодні найменші привілеї слід постійно використовувати в різних місцях і типах ресурсів, а також на мережевому та прикладному рівнях, використовуючи контекст безпеки та ідентифікуючі дані. Однак традиційно користувачі та їх пристрої отримували широкий доступ до мереж (сьогодні вважається, що можливість відправляти мережеві пакети в систему є привілеєм і керувати нею необхідно відповідним чином [6]), а застосунки використовували контроль доступу лише за допомогою перевірки автентичності (автентифікації). Грамотно забезпечуваний контроль доступу (наприклад, використання контролю доступу на основі ролей (RBAC) для всіх співробітників, реалізація керування привілейованими ідентифікаційними даними (PIM – privileged identity management) для доступу до важливих систем тощо) допомагає усунути людську спокусу отримати доступ до обмежених ресурсів. Хоча концепція нульової довіри не визначає RBAC як кращу методологію керування доступом. Сьогодні й в майбутньому слід розглядати й інші технології, методології (наприклад, ту саму ABAC) для керування доступом. У цьому випадку важлива сама концепція мінімальних привілеїв та суворого контролю доступу. Також важливо, щоб фахівці з безпеки розробили відповідну стратегію керування ідентифікацією та доступом, щоб періодично переглядати та підтверджувати права доступу працівників, у тому числі з великими привілеями. Так, наприклад, співробітники, які мають адміністративний доступ до важливих застосунків і систем, можуть завдати шкоди компанії, якщо вони мають злий намір. Крім того, такі привілейовані користувачі часто стають мішенню для хакерів, які намагаються скомпрометувати їхні облікові дані з корисливою метою. У цьому випадку рішення PIM, якраз, дозволяють фахівцям з безпеки уважно стежити за діями зазначених користувачів та вимагати від них пред'явлення паролів щоразу для отримання доступу до важливих систем.

3. Перевіряйте та реєструйте весь трафік.

Мережі є досить важливим місцем в IT-інфраструктурі та забезпеченні безпеки, оскільки вони є сполучною ланкою між розподіленими компонентами та їх взаємодією один з одним. Саме з цієї причини цей принцип потребує перевірки та протоколювання мережевого трафіку. Дійсно, постійно перевіряючи, реєструючи та аналізуючи мережевий трафік, фахівці з безпеки можуть виявити аномальну поведінку користувачів або їхню підозрілу активність (наприклад, якщо користувач виконує великі завантаження або часто звертається до систем або записів, які зазвичай йому не потрібні для виконання повсякденних обов'язків). Технологія мережі з нульовою довірою спрощує передачу вмісту мережевого трафіку та журналів до інструментарію аналізу безпеки для більш глибокого дослідження. Інформація про мережевий трафік повинна бути доповнена системою нульової довіри (додані ідентифікаційні дані та відомості про пристрій) та передана у міжмережеві екрани нового покоління, засоби мережевого моніторингу та SIEM (керування інформацією та подіями безпеки), щоб підвищити їхню здатність приймати рішення щодо виявлення, оповіщення та реагування. Важливо відзначити, що системи нульової довіри повинні не тільки широко вивчати та реєструвати метадані мережевого трафіку, але бути більш уважними при аналізі вмісту мережного трафіку через витрати на обробку та зберігання.

Дані принципи, на думку фахівців у галузі інформаційної безпеки, зазвичай вважаються основними і важливими [6] і повинні дотримуватися в будь-якій реалізації концепції нульової довіри.

Звичайно, як уже зазначалося, значний вплив на галузь інформаційної безпеки в цілому, і концепцію нульової довіри зокрема, зробив вихід у 2020 р. публікації NIST про архітектуру нульової довіри [7] та пов'язаний з нею проєкт NCCoE [4].

З точки зору NIST, *нульова довіра* являє собою набір концепцій та ідей, розроблених для мінімізації невизначеності в застосуванні точних рішень щодо доступу з найменшими привілеями для кожного запиту в інформаційних системах і службах, коли мережу вважають скомпрометованою. Архітектура нульової довіри (ZTA) – це план кібербезпеки підприємства, який використовує концепції нульової довіри та охоплює зв’язки компонентів, планування робочого процесу та політики доступу. Архітектура нульової довіри розробляється та розгортається з дотриманням наступних основних принципів нульової довіри [7]:

1. *Усі джерела даних і обчислювальні послуги вважаються ресурсами*. Мережа може складатися з кількох класів пристроїв. Також підприємство може ухвалити рішення вважати пристрої, що належать особисто співробітнику, ресурсами, якщо вони можуть отримати доступ до ресурсів, що належать підприємству.

2. *Усі комунікації захищаються незалежно від розташування мережі*. Розташування в мережі саме по собі не означає довіри. Довіра не повинна надаватися автоматично на основі того, що пристрій знаходиться в мережевій інфраструктурі підприємства. Усі комунікації повинні здійснюватися найбільш безпечним способом, забезпечувати конфіденційність та цілісність, а також автентифікацію джерела.

3. *Доступ до окремих ресурсів підприємства надається на основі кожного сеансу* (*лише на один сеанс*). Довіра до запитувача оцінюється перед наданням доступу. Доступ також має бути надано з найменшими привілеями, необхідними для виконання завдання.

4. *Доступ до ресурсів визначається динамічною політикою*, включаючи спостережуваний стан ідентичності клієнта, програми/сервісу та активу, який запитується, і може включати інші поведінкові атрибути та атрибути навколишнього середовища. Підприємство захищає ресурси, визначаючи, які ресурси вона має, хто є її членами (або здатність автентифікувати користувачів із об’єднаної спільноти) і який доступ до ресурсів потрібен цим членам. Для нульової довіри ідентифікатор клієнта може включати обліковий запис користувача (або ідентифікатор служби) і будь-які пов’язані атрибути, призначені підприємством цьому обліковому запису для автентифікації автоматизованих завдань. Стан активу запиту може включати такі характеристики пристрою, як встановлені версії програмного забезпечення,

мережеве розташування, час/дата запиту, поведінка, що спостерігалася раніше, і встановлені облікові дані. Політика – це набір правил доступу на основі атрибутів, які організація призначає суб'єкту, активу даних або програмі. Атрибути середовища можуть включати такі фактори, як мережеве розташування запитувача, час, повідомлення про активні атаки тощо. Правила доступу до ресурсів і дозволів на дії можуть відрізнятися залежно від чутливості ресурсу/даних. Принципи найменших привілеїв застосовуються для обмеження як видимості, так і доступності.

5. *Підприємство контролює та вимірює цілісність і стан безпеки всіх належних йому та пов'язаних з ним активів.* Жоден актив не є надійним. Підприємство оцінює стан безпеки активу під час оцінки запиту ресурсу. Підприємство має встановити безперервну діагностику та пом'якшення наслідків (CDM) або подібну систему для моніторингу стану пристроїв та застосунків і застосовувати виправлення за потреби.

6. *Усі автентифікації та авторизації ресурсів є динамічними та суворо контролюються перед тим, як доступ буде дозволений*. Це постійний цикл отримання доступу, сканування та оцінки загроз, адаптації та постійної переоцінки довіри у процесі безперервної взаємодії. Очікується, що підприємство, яке впроваджує ZTA, матиме системи *управління ідентифікацією, обліковими даними та доступом* (ICAM – Identity, Credential, and Access Management) і системи управління активами. Це включає використання *багатофакторної автентифікації* (MFA – multifactor authentication) для доступу до деяких або всіх ресурсів підприємства.

7. *Підприємство збирає якомога більше інформації про поточний стан активів, мережевої інфраструктури та комунікацій і використовує її для покращення стану безпеки*. Підприємство має збирати дані про стан безпеки активів, мережевий трафік і запити на доступ, обробляти ці дані та використовувати будь-яку отриману інформацію для покращення створення та застосування політики.

Ці принципи можна пов'язати з основними компонентами розширеної моделі нульової довіри Forrester. Оскільки підходи до нульової довіри NIST і Forrester відіграють важливу роль як керівництва (які поділяють основні принципові концепції нульової довіри за різними категоріями [39]) для забезпечення безпеки у відповідності до принципу нульової довіри на підприємстві.

У табл. 3 показано зіставлення основних компонент розширеної моделі нульової довіри Forrester з основними принципами нульової довіри NIST, що демонструє їх взаємозв'язок і дозволяє припустити, що будь-який з цих підходів може бути використаний як керівництво для забезпечення безпеки у відповідність до принципу нульової довіри.

Таблиця 3

Порівняння традиційної моделі безпеки та моделі нульової довіри

Forrester	**NIST**						
	Ресурси	Комунікаційна безпека	Безпека сеансу	Контроль доступу	Контроль безпеки активів	Безперервна автентифікація	Реєстрація інформації
Дані		√					
Мережа	√			√			
Люди	√	√	√	√		√	
Робочі навантаження	√			√		√	
Пристрої	√	√	√	√	√	√	
Видимість та аналітика							√
Автоматизація та оркестрування				√		√	

З основними принципами нульової довіри NIST також корелюють вісім принципів нульової довіри Національного центру кібербезпеки Великобританії (NCSC – National Cyber

Security Centre), які також можуть допомогти реалізувати власну архітектуру мережі з нульовою довірою у корпоративному середовищі, і які полягають у наступному [40]:

1. *Вивчіть свою архітектуру, включаючи користувачів, пристрої, послуги та дані*. Знання про кожен компонент своєї архітектури дозволить вам визначити, де знаходяться ваші ключові ресурси, які основні ризики для вашої архітектури, крім того, дозволить уникнути будь-яких помилок на пізньому етапі інтеграції успадкованих / застарілих сервісів, які не підтримують концепцію нульової довіри.

2. *З'ясуйте ідентифікаційні дані ваших користувачів, служб та пристроїв*. Ідентифікаційні дані (identity) можуть представляти користувача (людину), службу (процес) або пристрій. Кожен із них має бути однозначно ідентифікованим в архітектурі з нульовою довірою. Це один із найбільш важливих факторів при ухваленні рішення про те, чи слід комусь або чомусь надати доступ до даних або послуг.

3. *Оцініть поведінку ваших користувачів, стан пристроїв та сервісів*. Поведінка користувачів, стан служб або пристроїв є важливими показниками при забезпеченні впевненості в безпеці ваших систем. Можливість оцінювати поведінку користувачів, працездатність пристроїв та сервісів є ключовим аспектом в архітектурі нульової довіри.

4. *Використовуйте політики для авторизації запитів*. Кожен запит на отримання даних або послуг повинен бути авторизований відповідно до політики. Політики можуть допомогти полегшити управління ризиками під час обміну даними або послугами з гостьовими користувачами або партнерськими організаціями. Механізм політик є ключовим компонентом архітектури нульової довіри, який дозволяє забезпечити гнучкий, адаптований контроль доступу до запитуваних ресурсів.

5. *Автентифікація та авторизація всюди*. Рішення щодо автентифікації та авторизації повинні враховувати безліч ознак, таких як розташування пристрою, працездатність пристрою, особистість та статус користувача, щоб оцінити ризик, пов'язаний із запитом доступу.

6. *Зосередьте моніторинг на користувачах, пристроях та сервісах*. Моніторинг цих пристроїв, сервісів та поведінки користувачів допоможе визначити їхній стан. Моніторинг повинен бути пов'язаний з політиками, які були встановлені для забезпечення впевненості у їх правильному налаштуванні.

7. *Не довіряйте жодній мережі, включаючи власну*. Не довіряйте жодній мережі між пристроєм та сервісом (службою), до якого він звертається, включаючи локальну мережу. При передачі даних по мережі для доступу до даних або служб слід використовувати безпечний транспортний протокол, щоб бути впевненим у тому, що трафік захищений під час передачі і менш схильний до загроз. Архітектура нульової довіри змінює спосіб реалізації традиційних засобів захисту користувачів, таких як фільтрація шкідливих веб-сайтів та захист від фішингу, які можуть забезпечуватись різними рішеннями в архітектурі нульової довіри.

8. *Вибирайте сервіси (служби), створені на основі принципу нульової довіри*. Служби можуть не підтримувати нульову довіру і, отже, можуть вимагати додаткових ресурсів для інтеграції та збільшення витрат на підтримку. У таких випадках доцільно розглянути альтернативні продукти та служби, розроблені з урахуванням принципу нульової довіри. Використання продуктів, в яких застосовуються технології, що базуються на стандартах, дозволяє спростити інтеграцію та взаємодію між службами та постачальниками ідентифікаційних даних.

Ці вісім принципів, наприклад, використовували Oracle при розробці хмарної інфраструктури (OCI – Oracle Cloud Infrastructure) для надання клієнтам вбудованих функцій безпеки, що дозволяють швидко та ефективно захистити їх робочі навантаження [41]. Використання запропонованого Oracle рішення в майбутньому зможе допомогти багатьом організаціям, які хочуть бути більш гнучкими під час трансформації свого бізнесу, використовуючи загальнодоступну хмару для надання економічно ефективної інфраструктури, платформ та програмних послуг, впровадити модель безпеки з нульовою довірою до хмар.

Спираючись на важливий досвід міжнародних організацій та компаній в предметній області, що розглядається, можна зробити висновок, що представлений набір принципів має бути основним для реалізації будь-якої концепції нульової довіри. На наше глибоке переконання, концепція нульової довіри – це правильніший та ефективніший підхід до забезпечення безпеки підприємства. Кожен інтегрований у систему нульової довіри IT-компонент, що має необхідний рівень безпеки, підвищує її ефективність, корисність та сферу дії. І навпаки, кожен ізольований (не інтегрований) компонент створює додаткові труднощі, знижує ефективність системи нульової довіри та може перешкоджати забезпеченню безпеки. Зрозуміло, що немає єдино вірного рішення, спрямованого забезпечення нульового довіри. У зв'язку з цим керівники служб безпеки повинні враховувати інфраструктури, пріоритети, навички персоналу, бюджети та терміни при розробці своєї концепції нульової довіри. Через це концепція нульової довіри може здатися досить складною, але насправді масштаби її застосування допомагають значно вдосконалити систему безпеки та архітектуру підприємства.

В цілому ж, рішення інвестувати у нове рішення безпеки – складне та багатогранне питання. Оскільки інвестиції у безпеку важко оцінити кількісно, оскільки вони часто не приносять очевидної віддачі інвестицій. Особливо важливо враховувати вигоди для бізнес-процесів, співробітників та клієнтів, щоб мати можливість ухвалити обґрунтоване рішення [2].

Висновки

1. Щоб усунути недоліки, притаманні традиційній моделі безпеки (безпеки периметра), було запропоновано концепцію нульового довіри, як філософію, підхід і набір керівних принципів. Основна ідея даної концепції полягає в тому, що жодному учаснику інформаційного обміну не можна довіряти, а будь-який доступ до ресурсів організації є потенційною загрозою. Тому кожен доступ має контролюватись і верифікуватися. При цьому може надаватися повний доступ до служби/сервісу або лише до певних функцій або даних, для яких користувач має право. Причому перевірка не повинна виконуватися тільки на основі пароля, вона повинна враховувати безліч факторів і джерел інформації, таких як: пароль користувача, пристрій, час поточного розташування, права доступу тощо. Важливо визначити політику доступу і суворо її дотримуватися (при цьому політики доступу мають бути динамічними).

2. Планування приведення інфраструктури у відповідність до принципів нульової довіри неможливо здійснити частково або в рамках незначного доопрацювання відповідних інформаційних систем. Потрібна реорганізація інформаційної інфраструктури в цілому, а також інтеграція всіх аспектів, що забезпечують безпеку діяльності організації, щоб принципи нульової довіри показали свою ефективність.

3. Концепція нульової довіри продовжує розвиватися в міру того, як постачальники та організації зі стандартизації переглядають та вдосконалюють специфікації та реалізації нульової довіри, визнаючи це фундаментальним зрушенням у підході до інформаційної безпеки, кібербезпеки.

Список літератури:

1. Department of Defense. Global Information Grid Architectural Vision. Vision for a Net-Centric, Service-Oriented DoD Enterprise. Version 1.0 2007. URL: https://acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf. .

2. Buck C., Olenberger C., Schweizer A., Völter F., Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust // Computers & Security. 2021. 110. 102436.

3. Dhanarani A., Evans R., Loumi H., Lowenthal R., Lopes P., Mesaros M., Schaeumer B., Wahl P., Williams A., Zaidi N. Oracle Database Security a technical primer. Fifth edition. Version 5.0. 2023. URL: https://download.oracle.com/database/oracle-database-security-primer.pdf.

4. Kerman A., Borchert O., Rose S., Division E., Tan A. Implementing a zero trust architecture // National Institute of Standards and Technology. 2020. 17 p. URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf.

5. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.

6. Garbis J., Chapman J. W. Zero Trust Security: An Enterprise Guide. Berkeley, CA: Apress, 2021. 300 p.
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. Samaniego M., Deters R. Zero-trust hierarchical management in IoT // 2018 IEEE international congress on Internet of Things (ICIOT). IEEE, 2018. P. 88–95.
9. Ross R., Pillitteri V., Graubart, R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach // NIST Special Publication 800-160. Vol. 2. Revision 1. 2021. 310 p.
10. Zero Trust Security Market Size, Share & Trends Analysis Report By Deployment (Cloud, On-premises), By Security Type (Network, Endpoint), By Authentication, By Organization Size, By Application, By Region, And Segment Forecasts, 2023-2030. Zero Trust Security Market Size & Trends. URL: https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report.
11. Grand View Research. Zero Trust Security Market Growth & Trends. URL: https://www.grandviewresearch.com/press-release/global-zero-trust-security-market.
12. Gartner. Press Release. Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026. URL: https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026.
13. Fortinet. The State of Zero Trust. Report. 2023. URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-zero-trust.pdf.
14. Martinez J. Zero Trust Architecture: 2024 Complete Guide. URL: https://www.strongdm.com/zero-trust.
15. Shore M., Zeadally S., Keshariya A. Zero trust: the what, how, why, and when // Computer. 2021. Vol. 54. № 11. P. 26–35. https://doi.org/10.1109/MC.2021.3090018.
16. Kindervag J., Balaouras S., Mak K., Blackborow J. No More Chewy Centers: The Zero Trust Model Of Information Security. Forrester Research, Inc. 2016. URL: https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf.
17. Saltzer J. H., Schroeder M. D. The protection of information in computer systems // Proceedings of the IEEE. 1975. 63(9). P. 1278–1308.
18. Jericho Forum Commandments. Version 1.2. 2007. URL: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf.
19. 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.
20. Ward R., Beyer B. Beyondcorp: A new approach to enterprise security // login. 2014. 39(6). P. 6–11.
21. Osborn, B., McWilliams, J., Beyer, B., Saltonstall M. Beyondcorp: Design to deployment at google // login. 2016. 41(1). P. 28–35.
22. Cittadini L., Spear B., Beyer B., Saltonstall M. Beyondcorp: The access proxy // login. 2016. 41(4). P. 28–35.
23. Peck J., Beyer B., Beske, C. M., Saltonstall M. Migrating to BeyondCorp: maintaining productivity while improving security // login. 2017. 42(2). P. 49–55.
24. Escobedo V., Beyer B., Zyzniewski F., Saltonstall, M. BeyondCorp: the user experience // login. 2017. 42(3). P. 38–43.
25. King H., Janosko M., Beyer B., Saltonstall M. Beyondcorp 6: Building a healthy fleet // login. 2018. 43(3). P. 24–30.
26. Gonçalves G., O'Malley K., Beyer, B., Saltonstall M. BeyondCorp and the long tail of Zero Trust // login. 2023. 52423. URL: https://www.usenix.org/publications/loginonline/beyondcorp-and-long-tail-zero-trust.
27. Continuous Adaptive Risk and Trust Assessment (CARTA). URL: https://www.ssh.com/academy/iam/carta.
28. Sarkar S., Choudhary G., Shandilya S. K., Hussain A., Kim H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review // Sustainability. 2022. 14. 11213. https://doi.org/10.3390/su141811213.
29. Bayuk J. L. Stepping Through the InfoSec Program. ISACA. 2007. 238 p.
30. Erl T. Service-oriented architecture: concepts, technology, and design. Pearson Education India, 2005. 760 p.
31. Singhal A., Winograd T., Scarfone K. Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-95. 2007. 128 p.
32. Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. Version 2.0. 2023. URL: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.
33. Єсін В. І., Вілігура В. В., Сватовський І. І. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти // Радіотехніка. 2023. Вип. 214. С. 32–63. https://doi.org/10.30837/rt.2023.3.214.04.
34. Boyens J., Bartol N., Boyens J., Moorthy R., Paulsen C., Shankles S. A. Notional supply chain risk management practices for federal information systems // US Department of Commerce, National Institute of Standards and Technology. NISTIR 7622. 2012. 99 p.
35. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009. 2022. URL: https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf.
36. Temoshok D., Abruzzi C. Developing trust frameworks to support identity federations. US Department of Commerce, National Institute of Standards and Technology. NISTIR 8149. 2018. 34 p.

37. Holmes D., Burn J., Mellen A., Pollard J., Cerrato P., Cser A. OMB's Zero Trust Strategy: Government Gets Good. URL: https://www.forrester.com/blogs/ombs-zero-trust-strategy-government-gets-good/.

38. van der Meulen R. Build adaptive security architecture into your organization. 2017. URL: https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization.

39. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey // IEEE Access. 2022. Vol. 10. P. 57143-57179. doi: 10.1109/ACCESS.2022.3174679.

40. The National Cyber Security Centre. Zero trust architecture design principles. Guidance. Version 1.0. 2021. URL: https://www.ncsc.gov.uk/collection/zero-trust-architecture.

41. Toal P., Gopalan K. Approaching Zero Trust Security with Oracle Cloud Infrastructure. Version 1.2. Whitepaper. Oracle and/or its affiliates. 2022. URL: https://www.oracle.com/a/ocom/docs/whitepaper-zero-trust-security-oci.pdf.

Надійшла до редколегії 02.06.2024

Відомості про авторів:

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

Вілігура Владислав Вікторович – Харківський національний університет імені В.Н. Каразіна, викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

Узлов Дмитро Юрійович – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, в.о. декана факультету комп'ютерних наук; Україна; e-mail: dmytro.uzlov@karazin.ua; ORCID: https://orcid.org/0000-0003-3308-424X