УДК 004.056.53

д.т.н., проф. **Бобок І.І.** (НУ «ОП», Одеса)
д.т.н., проф. **Кобозєва А.А.** (ОНМА, Одеса)

DOI: http://doi.org/10.17721/2519-481X/2025/88-06

АРХІТЕКТУРА «НУЛЬОВОЇ ДОВІРИ» І ПЕРСПЕКТИВИ ЇЇ ВПРОВАДЖЕННЯ В ДЕРЖАВНИЙ СЕКТОР УКРАЇНИ

Сучасний етап розвитку інформаційних технологій супроводжується зростанням кібератак, що стають ключовим інструментом гібридної війни та впливають на безпеку державних інформаційних ресурсів. У контексті збройної агресії Росії проти України та масованих атак на критичну інфраструктуру актуальною є відмова від традиційної периметрової моделі кіберзахисту, яка в умовах розмитих мережевих кордонів і використання хмарних сервісів втрачає ефективність. Перспективним підходом визнано архітектуру нульової довіри ZTA, що ґрунтується на принципах «ніколи не довіряй, завжди перевіряй», мінімізації привілеїв і постійному моніторингу. Метою дослідження є аналіз можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж України з урахуванням нормативних вимог, обмежених ресурсів та підвищених ризиків у період гібридної агресії. У статті проведено огляд провідних міжнародних підходів, зокрема NIST SP 800-207, CISA Zero Trust Maturity Model та NCSC Design Principles, а також визначено бар'єри їх імплементації в українському контексті. Основні проблеми пов'язані з нормативними обмеженнями, застарілою інфраструктурою, браком кадрів і фінансовими ресурсами. Запропонована концептуальна модель передбачає поетапне впровадження ZTA на основі п'яти рівнів: управління ідентичностями, динамічний контроль доступу, мікросегментація мережі, захист даних та моніторинг із застосуванням аналітики поведінки. Модель інтегрує федеративне управління ідентичностями, багатофакторну автентифікацію, контекстну оцінку ризиків і централізовану платформу моніторингу. Очікуваним результатом є підвищення рівня кіберстійкості державних мереж без значного зниження продуктивності та забезпечення відповідності національним вимогам інформаційної безпеки.

Ключові слова: архітектура нульової довіри, zero trust, державні інформаційні системи, кібербезпека, гібридна війна, ідентифікація, мікросегментація, адаптивна автентифікація.

Вступ. Сучасний етап розвитку інформаційних технологій характеризується кардинальною трансформацією ландшафту кіберзагроз, особливо в умовах ескалації гібридної агресії. Події останніх років демонструють якісно новий рівень кіберзагроз, де кібератаки стають невід'ємною частиною воєнних дій та геополітичних протистоянь [1]. Державні мережі, які традиційно розглядаються як відносно захищені периметром системи, сьогодні стикаються з безпрецедентними за масштабом і складністю загрозами, що потребує фундаментального перегляду підходів до управління кібербезпекою.

Аналіз сучасного стану кібербезпеки державних мереж виявляє низку системних проблем в управлінні. По-перше, класична периметрова модель безпеки, що передбачає чіткий поділ на «внутрішні» та «зовнішні» загрози, втрачає ефективність в умовах розмитих кордонів мережної інфраструктури та зростаючої мобільності користувачів. По-друге, реактивний характер більшості систем управління кібербезпекою не дозволяє адекватно протидіяти складним багатоетапним атакам, характерним для державних акторів. По-третє, фрагментованість управління безпекою між різними відомствами та службами створює прогалини у загальній системі захисту [2].

Міжнародний досвід останніх років демонструє інтерес до архітектури «нульової довіри» (Zero Trust Architecture, ZTA) як до перспективного підходу до вирішення зазначених проблем. Концепція ZTA, що базується на принципі «ніколи не довіряй, завжди перевіряй», пропонує радикально інший підхід до управління кібербезпекою, де довіра не є статичним атрибутом, а динамічно оцінюється для кожного запиту на доступ до ресурсів.

Цей підхід є особливо актуальним для державних мереж, де критично важливо забезпечити безперервний контроль доступу до чутливої інформації та критичних систем.

Для державних мереж України, що функціонують в умовах повномасштабної агресії, питання інтеграції ZTA-підходів у систему управління кібербезпекою набуває особливої актуальності. Необхідність забезпечення безперервності функціонування критичних державних сервісів за умов постійного кіберпротистояння потребує не тільки технологічної модернізації, але й адаптації управлінських процесів до реалій архітектури нульової довіри.

Таким чином, актуальність даного дослідження обумовлена необхідністю наукового обґрунтування можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж з урахуванням умов гібридної агресії та воєнного часу.

Мета роботи. Мета роботи полягає в аналізі можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж України з урахуванням нормативних вимог, обмежених ресурсів та підвищених ризиків у період гібридної агресії.

Сучасний стан проблеми. В останнє десятиліття різні національні агенції кібербезпеки розробили власні підходи до впровадження Zero Trust Architecture у державних організаціях [3-5]. Аналіз цих підходів демонструє як загальні принципи, так і суттєві відмінності у методології та практичній реалізації.

Національний інститут стандартів та технологій США (NIST) у публікаціїSP 800-207 представив найбільш комплексний підхід до впровадження ZTA у державному секторі [6]. Документ визначає три фундаментальні принципи: «ніколи не довіряй, завжди перевіряй», що означає необхідність автентифікації та авторизації кожного запиту; принцип мінімальних привілеїв, згідно з яким доступ надається лише до необхідних ресурсів; та принцип «припускай порушення», що вимагає проектування системи з урахуванням можливості компрометації будь-якого елемента. SP 800-207 є фундаментальною методологією з високим рівнем деталізації і широкою застосовністю. Ключові переваги цього підходу включають комплексність архітектурних принципів, офіційну державну підтримку та універсальність для різних типів організацій. Серед обмежень слід виділити високу складність впровадження, значні вимоги до ресурсів та потенційну надмірність для невеликих державних установ з обмеженими можливостями IT.

Агенція з кібербезпеки і захисту інфраструктури США (CISA) розробила практико-орієнтовану модель — Zero Trust Maturity Model [7]. Ця модель визначає п’ять ключових доменів: ідентичність (Identity), пристрої (Devices), мережі (Networks), застосунки та робочі навантаження (Applications and Workloads), а також дані (Data). Для кожного домену передбачено чотири рівні зрілості: Traditional, Initial, Advanced та Optimal. Такий підхід забезпечує організаціям можливість планувати поетапний перехід до архітектури нульової довіри, виходячи з поточного рівня та цільових показників. Ключові переваги моделі включають наявність чітких індикаторів прогресу, структурованого підходу до розвитку можливостей та оптимізацію для державного сектору. Водночас модель має обмеження: орієнтація на нормативно-правову базу США, високі вимоги до ресурсів для досягнення вищих рівнів зрілості Advanced та Optimal, а також недостатнє опрацювання аспектів зручності використання.

Національний центр кібербезпеки Великобританії (NCSC) пропонує більш прагматичний підхід у своїй концепції Zero Trust Architecture Design Principles [8]. Британський підхід фокусується на п’яти ключових принципах: знання архітектури, яке передбачає глибоке розуміння існуючої інфраструктури, мережевих взаємодій та потоків даних; знання користувачів, яке вимагає ефективного управління ідентичністю, обліковими записами та привілеями; знання пристроїв, яке включає контроль та керування кінцевими точками, включаючи BYOD; знання сервісів, яке охоплює захист додатків, API та хмарних сервісів; принцип недовіри до мережі, який зобов’язує реалізувати наскрізне шифрування та мікросегментацію. Даний підхід характеризується прагматичності та гнучкістю застосування. Його переваги включають фокус на основних принципах безпеки, відносну

простоту розуміння та впровадження, а також можливість адаптації до різних організаційних контекстів. Однак цей підхід менш деталізований порівняно з американськими аналогами та потребує додаткової інтерпретації для конкретних умов впровадження.

Австралійський центр кібербезпеки (ACSC) пропонує практико-орієнтований фреймворк Essential Eight, спрямований на зниження ймовірності успішних кібератак за рахунок впровадження восьми ключових заходів захисту [9]. Даний підхід є набором мінімальних базових рекомендацій, що забезпечують захист від найбільш поширених загроз і вразливостей. Основні заходи включають: регулярне оновлення застосунків з метою усунення відомих вразливостей; своєчасне оновлення операційних систем; обов'язкова багатофакторна автентифікація для всіх критично важливих облікових записів; використання білих списків застосунків (whitelisting) для запобігання запуску несанкціонованого ПЗ; обмеження та контроль прав адміністрування; управління макросами з метою зниження ризику експлуатації вразливостей в документах; налаштування застосунків для мінімізації потенційних атак (наприклад, відключення небезпечних функцій); виконання регулярного резервного копіювання даних та перевірка відновлення. Основні переваги цього підходу полягають у простоті розуміння та реалізації, можливості поступового впровадження, оптимізації для базового захисту державних та комерційних структур. При цьому слід зазначити, що Essential Eight не є повноцінною архітектурною моделлю Zero Trust – в основному він орієнтований на мінімальний рівень захисту, недостатній для протидії цільовим APT-атакам і гібридним загрозам.

Специфічні проблеми впровадження ZTA в сучасних українських умовах. Впровадження ZTA у державних мережах України стикається з комплексом специфічних проблем, які потребують особливої уваги та адаптації міжнародних підходів до національних умов. Ці проблеми охоплюють нормативно-правову, технічну, економічну, організаційну та геополітичну сфери.

Для розуміння масштабу необхідних змін важливо порівняти переваги архітектури нульової довіри із традиційною периметровою моделлю, яка нині домінує в українських державних мережах. Таблиця 1 ілюструє ключові різницю між цими підходами.

Це порівняння демонструє, що перехід від периметрової моделі до ZTA вимагає фундаментального перегляду підходів до безпеки. Незважаючи на очевидні переваги архітектури нульової довіри, цей перехід пов'язаний із значними викликами в українському контексті.

Нормативно-правові виклики є однією з найбільш серйозних проблем для впровадження ZTA. Чинний Закон України «Про захист інформації в інформаційно-комунікаційних системах» [10] не містить спеціальних положень, які б регулювали принципи нульової довіри, що створює правову невизначеність при впровадженні відповідних технологій. Таким чином, необхідність гармонізації національного законодавства з вимогами Європейського союзу, включаючи GDPR [11] та директиву NIS2 [12], ускладнює процес адаптації ZTA-підходів. Відсутність національних стандартів ZTA призводить до фрагментарного та несистемного підходу до впровадження цих технологій у різних державних організаціях.

Вимоги Державної служби спеціального зв'язку та захисту інформації України, розроблені для традиційних периметрових моделей безпеки, не повністю відповідають принципам ZTA. Це створює необхідність адаптації існуючих процедур атестації та сертифікації інформаційних систем. Виникає також потенційний конфлікт між вимогами відкритості державних даних, закріпленими у Законі «Про доступ до публічної інформації» [13], та принципами обмеженого доступу, що лежать в основі архітектури нульової довіри.

Особливе занепокоєння викликають технічні обмеження, які є серйозною перешкодою для впровадження ZTA. Значна частина державних мереж побудована на застарілих технологіях, які не підтримують сучасні протоколи автентифікації та авторизації [14]. Відсутність сучасних засобів моніторингу та аналітики у більшості державних організацій унеможливлює реалізацію принципу неперервної верифікації доступу. Обмежена пропускна

спроможність каналів зв'язку, особливо у регіональних державних установах, створює додаткові труднощі застосування систем, які потребують інтенсивної мережевої взаємодії.

Кадрові проблеми посилюють технічну ситуацію [15]. Гостра нестача фахівців з кібербезпеки у державному секторі призводить до того, що багато організацій не мають достатнього експертного потенціалу для планування та реалізації проектів впровадження ZTA. Недостатній рівень знань про сучасні технології безпеки серед існуючих IT-фахівців потребує значних інвестицій у навчання та перепідготовку. Висока плинність кадрів у IT-підрозділах державних організацій, обумовлена низьким рівнем оплати праці в порівнянні з приватним сектором, створює додаткові труднощі для накопичення експертизи в галузі ZTA.

Таблиця 1

Порівняння периметрової моделі і Zero Trust Architecture

Критерій	Периметрова модель	Zero Trust Architecture
Модель довіри	Довіра – всередині периметра, недовіра – ззовні	Нікому не довіряй, завжди перевіряй
Принцип безпеки	Захист периметра	Захист кожного ресурсу
Автентифікація	Одноразова при вході до мережі	Неперервна для кожного запиту
Авторизація	Широкі права доступу всередині периметра	Мінімальні привілеї для кожного ресурсу
Сегментація	Груба сегментація по підмережам	Мікросегментація на рівні застосунків
Моніторинг	Фокус на периметрі	Моніторинг всіх взаємодій
Масштабуємість	Обмежена віддаленим доступом	Висока для розподілених середовищ
Адаптивність до загроз	Повільна реакція на внутрішні загрози	Швидке виявлення і реагування
Складність управління	Відносна проста	Висока, потребує автоматизації
Вартість впровадження	Низька для існуючих систем	Висока на початковому етапі
Сумісність з хмарними рішеннями	Обмежена	Висока
Захист від інсайдерських загроз	Слабка	Сильна

Економічні чинники є критичним обмеженням для впровадження ZTA. Обмежене фінансування IT-проектів у державному секторі, особливо в умовах воєнного часу, робить проблематичним виділення коштів на масштабні проекти модернізації безпекової інфраструктури. Висока вартість сучасних безпекових рішень, включаючи ліцензії на програмне забезпечення, обладнання та послуги інтеграції, часто перевищує бюджетні можливості державних організацій. Необхідність значних інвестицій у навчання персоналу створює додаткове фінансове навантаження на і без того обмежені IT-бюджети.

Проблеми державних закупівель додають додаткових труднощів до економічних викликів. Існуючі процедури державних закупівель, орієнтовані на стандартні товари та послуги, погано адаптовані для придбання інноваційних рішень безпеки. Відсутність спеціалізованих технічних вимог для ZTA-рішень у типовій тендерній документації призводить до закупівлі неадекватних чи неповних рішень. Обмежений вибір локальних постачальників, здатних надати комплексні ZTA-рішення, створює залежність від закордонних виробників, що є неприпустимим для державного сектору і критично важливої інфраструктури, та ускладнює процес закупівель.

Організаційні виклики включають культурні бар'єри та проблеми міжвідомчої взаємодії. Традиційний підхід до управління IT-безпекою, що базується на периметровій моделі, глибоко вкорінений в організаційній культурі державних установ. Опір змінам з боку персоналу, особливо серед керівного складу, що не має достатнього розуміння сучасних загроз кібербезпеці, уповільнює процес впровадження нових підходів. Недостатнє розуміння переваг ZTA на управлінському рівні призводить до низького пріоритету відповідних проектів у стратегічному плануванні організацій.

Складність міжвідомчої взаємодії створює додаткові перешкоди системного впровадження ZTA. Різні державні органи мають різний рівень готовності до впровадження нових технологій, що ускладнює координацію спільних проектів безпеки. Відсутність єдиного підходу до управління кібербезпекою на міжвідомчому рівні призводить до фрагментації зусиль та неефективного використання ресурсів.

Геополітичні чинники додають унікальні виклики для запровадження ZTA в умовах України. Військовий стан створює особливі вимоги до безпеки, які не завжди сумісні зі стандартними підходами до впровадження нових технологій. Необхідність забезпечення безперервності роботи критично важливих систем в умовах постійних загроз обмежує можливості масштабних змін інфраструктури. Постійні кібератаки на державну інфраструктуру вимагають фокусування ресурсів на оперативному реагуванні, що відволікає від довгострокових проектів модернізації.

Вимоги до імпортозаміщення в критично важливих системах створюють додаткові обмеження щодо вибору технологічних рішень. Необхідність використання вітчизняних чи союзних технологій може обмежувати доступ до найбільш передових ZTA-рішень, представлених на світовому ринку.

Таким чином, для успішного впровадження ZTA у державному секторі України необхідна розробка комплексного підходу, який би враховував специфіку національних умов та поетапну стратегію реалізації.

Для подолання виявлених проблем потрібна розробка комплексного підходу, який враховуватиме специфіку українських умов та забезпечуватиме поетапну стратегію впровадження ZTA. Такий підхід має включати адаптацію міжнародних методологій до національного контексту, розробку відповідної нормативної бази, створення програм підготовки кадрів, оптимізацію процедур закупівлі та забезпечення міжвідомчої координації. Особливу увагу слід приділити забезпеченню сумісності з існуючими системами та поетапному переходу від традиційних периметрових моделей до архітектури нульової довіри.

Адаптована модель ZTA для українських держаних інформаційно-комунікаційних систем. Враховуючи специфічні умови та обмеження, виявлені у попередньому розділі, пропонується адаптована модель ZTA, яка враховує особливості українського державного

сектору. Ця модель базується на принципах міжнародних стандартів, але адаптована до національних умов, включаючи нормативно-правові вимоги, технічні обмеження та економічні реалії.

Запропонована архітектура будується довкола п’яти основних компонентів, кожен з яких адаптований до умов українських державних мереж:

Рівень керування ідентичністю та доступом є фундаментом архітектури. Цей рівень забезпечує централізоване керування користувачами, їх атрибутами та правами доступу. Для державних організацій пропонується інтеграція з існуючими системами управління персоналом та адаптація до вимог українського законодавства щодо захисту персональних даних. Компонент включає підсистеми багатофакторної автентифікації, керування життєвим циклом користувачів та федеративного доступу між різними державними організаціями.

Рівень контролю доступу до ресурсів забезпечує динамічне ухвалення рішень щодо надання доступу на основі комплексного аналізу контекстної інформації. Цей рівень включає чотири ключові компоненти:

— механізм поведінкової аналітики – аналізує патерни поведінки користувачів та виявляє аномалії у їхніх діях;
— аналізатор пристроїв та мережного контексту – оцінює характеристики пристроїв, розташування підключення та параметри мережного середовища;
— система класифікації даних – забезпечує відповідність різним рівням таємності інформації та інтеграцію із системами класифікації державних даних;
— підсистема геополітичного контексту – унікальний компонент, який аналізує поточну геополітичну обстановку, рівень кіберзагроз, статус інформаційних конфліктів та інтегрується з національними системами моніторингу загроз для коригування рівнів довіри у режимі реального часу.

Рівень мікросегментації мережі забезпечує ізоляцію ресурсів та контроль трафіку на гранулярному рівні. Компонент включає програмно-визначені периметри, динамічні правила фільтрації трафіку та системи виявлення аномалій. Для державних мереж передбачено сумісність із існуючими системами класифікації трафіку та вимогами до аудиту мережевих підключень.

Рівень захисту даних забезпечує наскрізне шифрування, класифікацію та контроль доступу до даних незалежно від їхнього розташування. Компонент включає системи запобігання витоку даних DLP, управління правами на цифрову інформацію та забезпечення цілісності даних. Для українських державних організацій передбачено інтеграцію з національними системами електронного документообігу та відповідність вимогам законодавства про захист державної таємниці.

Рівень моніторингу та аналітики забезпечує безперервний моніторинг безпеки, аналіз поведінки користувачів та автоматичне реагування на загрози. Компонент включає системи збирання та кореляції подій безпеки, машинного навчання для виявлення аномалій та автоматизованого реагування на інциденти. Для державного сектору передбачено інтеграцію з національними системами моніторингу кібербезпеки та відповідність вимогам до звітності про інциденти.

Адаптація міжнародних підходів до українських умов ґрунтується на кількох ключових принципах:

1. Принцип поетапності передбачає поступовий перехід від існуючих периметрових моделей до архітектури нульової довіри без порушення безперервності роботи критично важливих систем.
2. Принцип сумісності забезпечує інтеграцію з існуючими системами та технологіями, мінімізуючи необхідність повної заміни інфраструктури.
3. Принцип відповідності вимагає адаптації до національних нормативно-правових вимог та стандартів безпеки.

4. Принцип економічної ефективності передбачає оптимізацію витрат за впровадження та експлуатацію системи з урахуванням бюджетних обмежень державного сектора.
5. Принцип масштабованості забезпечує можливість розширення системи на різні рівні державного управління від місцевих адміністрацій до центральних органів влади.
6. Принцип стійкості до загроз враховує специфіку геополітичної ситуації та вимоги щодо забезпечення безпеки в умовах підвищених кіберзагроз.

Технічна реалізація запропонованої архітектури включає декілька ключових компонентів:

— *Центральний контролер політик* забезпечує централізоване управління правилами доступу та безпековими політиками. Цей компонент інтегрується з існуючими системами управління та забезпечує однакове застосування політик безпеки у всіх підключених організаціях.

— *Точки застосування політик* розгортаються на різних рівнях мережної інфраструктури та забезпечують контроль доступу до ресурсів відповідно до рішень центрального контролера. Ці компоненти можуть бути реалізовані як програмні агенти, інтегровані в існуючі системи або як спеціалізовані апаратні пристрої.

— *Система керування ідентичністю* забезпечує автентифікацію користувачів та керування їх атрибутами. Для державного сектора передбачена інтеграція із системами електронної ідентифікації громадян та державних службовців.

— *Система контекстної аналітики* забезпечує аналіз ризиків та прийняття рішень на основі поведінкових патернів, характеристик пристроїв та мережевого контексту.

Проводячи порівняльний аналіз запропонованої адаптованої моделі ZTA з розглянутими вище аналогами, слід підкреслити її фундаментальні відмінності.

Ключова відмінність полягає у додаванні компонента геополітичного контексту, який враховує підвищені кіберзагрози та вимоги до забезпечення національної безпеки. На відміну від базової моделі NIST, архітектура, що пропонується, включає спеціалізовані механізми для роботи з класифікованою інформацією різних рівнів секретності та інтеграцію з національними системами криптографічного захисту. Крім того, в моделі додаються специфічні компоненти для державного сектора, такі як федеративне управління ідентичністю між різними державними організаціями, інтеграція із системами електронного документообігу та відповідність вимогам національного законодавства щодо захисту персональних даних. Модель також передбачає поетапний перехід із урахуванням бюджетних обмежень державного сектора.

Етапи впровадження адаптованої моделі. Перехід від традиційної периметрової моделі до архітектури нульової довіри потребує структурованого підходу, який мінімізує ризики порушення роботи існуючих систем та забезпечує поетапне підвищення рівня безпеки. Запропонована модель впровадження складається з п’яти незалежних етапів, кожен із яких представляє самостійну цінність і може бути реалізований незалежно від інших.

Для забезпечення ефективного управління процесом впровадження запропонованої моделі визначені критерії успішності кожного етапу та оцінки їх кількісних характеристик, при цьому обґрунтування і уточнення конкретних виразів останніх є результатами дослідження авторів, які зараз готуються до друку, тому не приводяться детально в цій роботі.

Етап 1: Інвентаризація та аналіз існуючої інфраструктури. Перший етап фокусується на детальному аналізі поточного стану інформаційних систем та мережевої інфраструктури державної організації. Мета етапу полягає у створенні повної карти цифрових активів,

розумінні потоків даних та ідентифікації критично важливих ресурсів, що потребують пріоритетного захисту.

Інвентаризація включає автоматизоване сканування мережної інфраструктури з метою виявлення всіх підключених пристроїв, серверів, робочих станцій і мережного устаткування. Аналіз програмних активів охоплює всі встановлені застосунки, операційні системи, бази даних та мережеві послуги. Особлива увага приділяється виявленню застарілих систем, які можуть становити загрозу безпеці.

Картування потоків даних включає аналіз всіх інформаційних обмінів між системами, виявлення критично важливих даних та шляхів їх обробки. Проводиться класифікація даних щодо рівня конфіденційності відповідно до вимог українського законодавства. Аналізуються існуючі механізми захисту даних та виявляються прогалини у їх покритті.

Оцінка ризиків безпеки включає аналіз вразливостей у існуючих системах, моделювання потенційних загроз та оцінку можливої шкоди від їх реалізації. Проводиться аналіз відповідності існуючих заходів безпеки вимогам національних стандартів та найкращих міжнародних практик.

Результатом першого етапу є створення детальної карти цифрової інфраструктури, реєстру критично важливих активів, класифікації даних за рівнями конфіденційності та приоритизованого списку загроз безпеці. Ця інформація є основою для планування наступних етапів впровадження ZTA.

Успішність першого етапу оцінюється за повнотою та якістю проведеної інвентаризації та аналізу.

Критерій повноти інвентаризації передбачає виявлення 93–97% всіх цифрових активів організації, включаючи сервери, робочі станції, мережне устаткування й програмні системи. Якість інвентаризації оцінюється за точністю класифікації активів, коректністю визначення їх критичності та за повнотою опису залежностей між системами.

Критерій якості аналізу потоків даних передбачає картування всіх критично важливих інформаційних обмінів та визначення шляхів обробки конфіденційної інформації. Успішність оцінюється за відповідністю класифікації даних вимогам національного законодавства та повноті виявлення потенційних точок витоку інформації.

Критерій ефективності оцінки ризиків включає виявлення всіх критичних вразливостей у існуючих системах та пріоритизацію загроз відповідно до їх потенційного впливу на організацію. Успішність етапу підтверджується створенням детального плану усунення виявлених вразливостей та чітким розумінням поточного рівня ризику.

Етап 2: Впровадження централізованого управління ідентичністю. Другий етап фокусується на створенні єдиної системи управління ідентичності та доступом, яка стане фундаментом для всіх наступних компонентів архітектури нульової довіри. Мета етапу полягає в централізації управління користувачами, стандартизації процедур автентифікації та створенні основи для застосування принципу мінімальних привілеїв.

Розгортання системи управління ідентичністю починається із створення центрального репозиторію користувачів, який інтегрується з існуючими системами управління персоналом. Передбачається інтеграція із національними системами електронної ідентифікації для забезпечення відповідності вимогам законодавства.

Впровадження багатофакторної автентифікації включає розгортання додаткових факторів автентифікації, крім традиційних паролів. Система підтримує різні методи автентифікації, включаючи SMS-коди, мобільні застосунки, апаратні токени та біометричні дані. Для державного сектора передбачена інтеграція із системами електронного підпису та відповідність вимогам до криптографічного захисту.

Створення системи управління правами доступу включає визначення ролей та дозволів відповідно до організаційної структури та функціональних обов’язків користувачів. Система забезпечує автоматичне призначення прав доступу на основі посадових інструкцій та автоматичне відкликання доступу при зміні статусу користувача. Передбачається інтеграція

із системами управління життєвим циклом користувачів для автоматизації процесів надання та відкликання доступу.

Результатом другого етапу є створення централізованої системи управління ідентичністю, впровадження багатофакторної автентифікації для всіх користувачів, створення структурованої системи управління правами доступу та забезпечення єдиного входу до корпоративних застосунків. Цей етап значно підвищує рівень безпеки організації та створює основу для наступних етапів запровадження ZTA.

Успішність другого етапу оцінюється за ефективністю впровадження централізованого управління ідентичністю та якістю інтеграції з існуючими системами.

Критерій охоплення користувачів передбачає включення до системи управління ідентичністю не менше 100% активних користувачів організації з коректним визначенням їх ролей та дозволів.

Критерій ефективності багатофакторної автентифікації передбачає впровадження додаткових факторів автентифікації для всіх користувачів з привілейованим доступом і для 78–85% звичайних користувачів. Успішність оцінюється за зниженням кількості інцидентів, пов’язаних з компрометацією облікових записів, та відповідністю вимогам національних стандартів безпеки.

Критерій якості управління правами доступу включає автоматизацію процесів надання та відкликання доступу для 90–95% користувачів організації. Успішність підтверджується відповідністю принципу мінімальних привілеїв та відсутністю надлишкових прав доступу у користувачів.

Етап 3: Реалізація динамічного контролю доступу. Третій етап фокусується на створенні системи динамічного контролю доступу, яка приймає рішення про надання доступу на основі аналізу багатьох факторів ризику. Мета етапу полягає у переході від статичних правил доступу до динамічної оцінки ризику та адаптивного контролю доступу.

Розгортання системи оцінки ризиків включає створення механізмів аналізу контекстної інформації кожного запиту доступу. Система аналізує поведінкові патерни користувачів, характеристики пристроїв, розташування, час доступу та інші контекстні фактори. Для державного сектора передбачено інтеграцію із системами класифікації інформації та облік вимог до різних рівнів секретності.

Використання адаптивної автентифікації забезпечує застосування додаткових заходів автентифікації залежно від рівня ризику. Система може вимагати додаткову автентифікацію для доступу до критично важливих ресурсів у випадку виявлення аномальної поведінки або запиту на доступ з невідомих пристроїв. Передбачається інтеграція із системами аналізу поведінки користувачів для автоматичного виявлення аномалій.

Створення системи контекстного аналізу включає впровадження механізмів збирання та аналізу інформації про контекст доступу. Система аналізує мережеве оточення, характеристики пристроїв, геолокацію та часові патерни доступу. Для державних організацій передбачена інтеграція із системами моніторингу безпеки та відповідність вимогам до аудиту доступу.

Впровадження динамічних політик доступу забезпечує автоматичну зміну правил доступу залежно від зміни безпекових умов. Система може автоматично обмежувати доступ при виявленні загроз, змінювати вимоги до автентифікації залежно від рівня ризику та застосовувати додаткові заходи захисту для критично важливих ресурсів.

Результатом третього етапу є створення системи динамічного контролю доступу, впровадження адаптивної автентифікації, створення механізмів контекстного аналізу та застосування динамічних безпекових політик. Цей етап значно підвищує здатність організації до виявлення та запобігання загрозам безпеки. Саме на цьому етапі активується підсистема геополітичного контексту рівня контролю доступу до ресурсів.

Успішність третього етапу оцінюється за ефективністю системи динамічного контролю доступу та якістю оцінки ризиків.

Критерій точності оцінки ризиків передбачає досягнення не менше 90% точності у визначенні рівня ризику для запитів доступу з мінімальною кількістю помилкових спрацьовувань.

Критерій ефективності адаптивної автентифікації включає автоматичне застосування додаткових заходів автентифікації для 95–97% високоризикових запитів доступу. Успішність оцінюється за зниженням кількості успішних атак на системи організації та відповідністю часу відгуку вимогам користувачів.

Критерій якості контекстного аналізу передбачає облік не менше п’яти різних факторів ризику при прийнятті рішень про доступ, включаючи поведінкові патерни, характеристики пристроїв та мережевий контекст. Успішність підтверджується підвищенням здатності системи до виявлення аномальної поведінки та запобіганням несанкціонованому доступу.

Етап 4: Впровадження мікросегментації мережі. Четвертий етап фокусується на створенні мікросегментованої мережевої архітектури, яка забезпечує ізоляцію ресурсів та контроль трафіку на гранулярному рівні. Мета етапу полягає у заміні традиційної моделі «довіри всередині периметра» на модель «нульової довіри до мережі».

Впровадження програмно-визначуваних периметрів включає створення безпечних каналів зв’язку між авторизованими користувачами та ресурсами. Система створює індивідуальні зашифровані тунелі для кожного користувача, забезпечуючи ізоляцію трафіку та приховування ресурсів від неавторизованих користувачів. Для державного сектору передбачено інтеграцію з національними системами криптографічного захисту та відповідність вимогам до захисту державної таємниці.

Створення системи мікросегментаціїпередбачає логічний поділ мережної інфраструктури на невеликі сегменти з контрольованою взаємодією між ними. Кожен сегмент містить мінімальний набір ресурсів, необхідні виконання конкретних наперед визначених функцій. Система забезпечує детальний контроль трафіку між сегментами та автоматичне застосування політик безпеки.

Впровадження системи інспекції трафіку забезпечує глибокий аналіз всіх мережевих з’єднань та виявлення потенційних загроз. Система аналізує вміст трафіку, виявляє аномальні патерни та автоматично блокує підозрілі з’єднання. Для державних мереж передбачено інтеграцію з національними системами моніторингу кібербезпеки та відповідність вимогам до звітності про мережеві інциденти.

Розгортання системи автоматичного реагування включає створення механізмів швидкого реагування на виявлені загрози. Система може автоматично ізолювати скомпрометовані сегменти, блокувати підозрілий трафік та застосовувати додаткові заходи захисту. Передбачається інтеграція із системами управління інцидентами та відповідність вимогам до процедур реагування на кіберінциденти.

Результатом четвертого етапу є створення мікросегментованої мережевої архітектури, впровадження програмно-визначуваних периметрів, створення системи глибокої інспекції трафіку та автоматичного реагування на загрози. Цей етап значно підвищує здатність організації до локалізації загроз та запобігання їх поширенню.

Успішність четвертого етапу оцінюється за ефективністю мікросегментації мережі та якістю контролю трафіку.

Критерій повноти сегментації передбачає створення ізольованих сегментів для всіх критично важливих ресурсів з контрольованою взаємодією між ними.

Критерій ефективності контролю трафіку включає інспекцію 100% мережевого трафіку з автоматичним виявленням та блокуванням підозрілих з’єднань. Успішність оцінюється за зниженням часу виявлення загроз і підвищенням ефективності їх локалізації.

Критерій якості ізоляції загроз передбачає автоматичне обмеження поширення загроз у межах одного сегмента мережі. Успішність підтверджується відсутністю випадків поширення шкідливого коду за межі скомпрометованого сегмента.

Етап 5: Впровадження комплексного моніторингу та аналітики. П’ятий етап фокусується на створенні комплексної системи моніторингу безпеки та аналітики, яка

забезпечує безперервний контроль стану безпеки та автоматичне виявлення загроз. Мета етапу полягає у створенні системи ситуаційної поінформованості про стан кібербезпеки та забезпечення швидкого реагування на інциденти.

Впровадження системи збору та кореляції подій включає створення централізованої платформи для агрегації безпековихданих з усіх компонентів інфраструктури. Система збирає логи безпеки, події автентифікації, мережеву телеметрію та іншу інформацію щодо стану безпеки. Для державного сектору передбачено інтеграцію з національними системами моніторингу та відповідність вимогам до зберігання та обробки даних про безпеку.

Створення системи поведінкової аналітики передбачає використання алгоритмів машинного навчання для аналізу поведінки користувачів та виявлення аномалій. Система створює базові профілі нормальної поведінки для кожного користувача та автоматично виявляє відхилення, які можуть вказувати на компрометацію облікових записів або інсайдерські загрози. Передбачається адаптація алгоритмів до специфіки державного сектора та інтеграція із системами управління персоналом.

Впровадження системи аналізу загроз включає створення механізмів автоматичного виявлення та класифікації кіберзагроз. Система аналізує індикатори компрометації, зіставляє їх із базами даних загроз і автоматично визначає рівень ризику. Для державного сектору передбачено інтеграцію з національними системами обміну інформацією про загрози та відповідність вимогам до класифікації інцидентів.

Створення системи автоматизованого реагування включає розробку сценаріїв автоматичного реагування на різні типи кіберінцидентів. Система може автоматично блокувати скомпрометовані облікові записи, ізолювати заражені пристрої, застосовувати додаткові заходи автентифікації та повідомляти служби безпеки про критичні інциденти. Передбачається інтеграція із системами управління інцидентами та відповідність процедурам реагування на кіберінциденти.

Результатом п’ятого етапу є створення комплексної системи моніторингу безпеки, запровадження поведінкової аналітики, створення системи аналізу загроз та автоматизованого реагування. Цей етап завершує створення повноцінної архітектури нульової довіри та забезпечує організацію сучасними засобами захисту від кіберзагроз.

Успішність п’ятого етапу оцінюється за ефективністю системи моніторингу та якістю аналітики безпеки.

Критерій повноти моніторингу передбачає збирання та аналіз даних про безпеку від усіх компонентів інфраструктури зі створенням єдиної картини стану безпеки.

Критерій ефективності виявлення загроз включає автоматичне виявлення щонайменше 95% відомих типів загроз із мінімальною кількістю помилкових спрацьовувань. Успішність оцінюється за зниженням часу виявлення інцидентів і підвищенням точності їх класифікації.

Критерій якості автоматизованого реагування передбачає автоматичне застосування відповідних заходів реагування для 80–85% виявлених інцидентів. Успішність підтверджується зниженням часу реагування на загрози та підвищенням ефективності їх нейтралізації.

Загальний критерій успішності впровадження запропонованої моделі передбачає досягнення вимірюваного підвищення рівня безпеки організації, відповідності вимогам національних стандартів безпеки та забезпечення безперервності роботи критично важливих систем протягом усього процесу впровадження.

Оцінка ризиків впровадження. Впровадження запропонованої моделі пов’язане з певними ризиками, які умовно можуть бути класифіковані на декілька груп, а саме: технічні, безпекові, організаційні та економічні. Тут ми пропонуємо спочатку розглянути технічні та безпекові ризики, як такі, які мають найбільше значення з нашої точки зору при імплементації архітектури безпеки.

До технічних ризиків належать:

— *Ризик сумісності* (високий рівень). Впровадження ZTA може призвести до конфліктів із існуючими системами та технологіями. Для мінімізації ризику пропонується

поетапний підхід із попереднім тестуванням сумісності та розробкою перехідних рішень.

— *Ризик продуктивності* (середній рівень). Додаткові рівні перевірки та шифрування можуть знизити продуктивність системи. Рекомендується використання апаратного прискорення криптографічних операцій та оптимізація алгоритмів прийняття рішень.

— *Ризик складності управління* (високий рівень). Збільшення кількості політик безпеки може призвести до помилок конфігурації. Пропонується розробка автоматизованих інструментів управління та навчання персоналу.

До безпекових ризиків належать:

— *Ризик виникнення нових векторів атак* (середній рівень). Складність системи може створити нові вразливості. Рекомендується регулярний аудит безпеки та тестування на проникнення.

— *Ризик відмови в обслуговуванні* (високий рівень). Централізовані компоненти можуть бути точкою відмови. Пропонується створення резервованих систем та планів аварійного відновлення.

— *Ризик компрометації центральних компонентів* (високий рівень). Атака на центральні компоненти може спричинити компрометацію всієї системи. Потрібні додаткові заходи захисту критично важливих компонентів.

Для мінімізації виявлених ризиків пропонується комплексний підхід, що включає технічні рішення (дублювання критично важливих компонентів, автоматизація процесів, використання відкритих стандартів), організаційні заходи (навчання персоналу, створення центру компетенцій, розробка процедур управління змінами) та економічні інструменти (поетапне фінансування, залучення міжнародних грантів).

Реалізація запропонованих заходів дозволить знизити загальний рівень ризиків впровадження з високого до прийнятного рівня та забезпечить успішний перехід до архітектури нульової довіри в українських державних мережах.

Висновки. Проведене дослідження проблем впровадження архітектури нульової довіри у державному секторі України та розроблені пропозиції щодо їх вирішення дозволяють зробити наступні висновки.

Аналіз сучасних кіберзагроз та вразливостей традиційних периметрових моделей безпеки демонструє критичну необхідність переходу українських державних організацій до архітектури нульової довіри. Традиційна модель «довіри всередині периметра» демонструє свою неефективність в умовах сучасних кібератак, особливо з огляду на специфіку геополітичної ситуації в Україні.

Пряме застосування міжнародних стандартів та методологій ZTA в українських умовах неможливе без їх суттєвої адаптації до національних особливостей. Розроблена адаптована модель враховує специфіку українського контексту та включає унікальні компоненти, які не представлені у базових міжнародних стандартах.

Ключовим нововведенням є включення компонента геополітичного контексту, що аналізує поточну геополітичну ситуацію та коригує рівні довіри залежно від зовнішніх загроз. Модель також передбачає інтеграцію з національними системами криптографічного захисту, електронного документообігу та класифікації державної інформації.

Перехід до архітектури нульової довіри забезпечить державним структурам значні переваги: підвищення адаптивності до нових видів атак, покращення можливостей

моніторингу та реагування на інциденти, посилення захисту від інсайдерських загроз, а також підвищення загального рівня кібербезпеки критично важливої інфраструктури.

ЛІТЕРАТУРА:

1. Zhou Z., Duan D., Xu H. Zero-Trust Zero-Communication Defence against Hybrid Cyberattacks in Distributed Energy Resources Using Mean Field Reinforcement Leaning. Energies. 2024. 17(20). 5057.
2. Nisha T N, Dhanya Pramod, Ravi Singh. Zero trust security model: Defining new boundaries to organizational network. *Proceedings of the 2023 15th International Conference on Contemporary Computing (IC3-2023)*. New York, NY, USA, 2023. P. 603–609.
3. Executive Order No. 14028, 3 C.F.R. 14028 (2021). https://public-inspection.federalregister.gov/2021-10460.pdf (дата звернення: 20.06.2025).
4. The Department of Homeland Security. Zero Trust Implementation Strategy. URL: https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf (дата звернення: 20.06.2025).
5. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*. 2023. 11. С. 19487–19511.
6. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. 59 p.
7. Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model, Version 2.0. URL: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (дата звернення: 20.06.2025).
8. The National Cyber Security Centre. Zero trust architecture design principles. URL: https://www.ncsc.gov.uk/collection/zero-trust-architecture (дата звернення: 20.06.2025).
9. Australian Cyber Security Centre. Essential Eight. URL: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight (дата звернення: 20.06.2025).
10. Про захист інформації в інформаційно-комунікаційних системах (назва Закону із змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020): Закон України. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
11. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/reglament-es-2016679.pdf (дата звернення: 20.06.2025).
12. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22 (дата звернення: 20.06.2025)
13. Про доступ до публічної інформації: Закон України. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.
14. Худолій А. Кібербезпека: сучасні виклики перед Україною. *Acta De Historia & Politica: Saeculum XXI*. 2019. Вип. 1. С. 138–146.
15. Євсюкова О.В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. *Державне управління: удосконалення та розвиток*. 2021. Вип. 2. URL: https://doi.org/10.32702/2307-2156-2021.2.2 (дата звернення: 20.06.2025).

REFERENCES:

1. Zhou, Z., Duan, D., and Xu H. (2024). "Zero-Trust Zero-Communication Defence against Hybrid Cyberattacks in Distributed Energy Resources Using Mean Field Reinforcement Leaning", *Energies*, 17(20), 5057. Available at: https://doi.org/10.3390/en17205057
2. Nisha T N, DhanyaPramod, and Ravi Singh. (2023). "Zero trust security model: Defining new boundaries to organizational network", *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing (IC3-2023)*. New York, NY, USA, pp. 603–609.
3. Executive Order No. 14028, 3 C.F.R. 14028 (2021). Available at: https://public-inspection.federalregister.gov/2021-10460.pdf (Accessed: 20.06.2025).
4. The Department of Homeland Security. *Zero Trust Implementation Strategy*. Available at: https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf (Accessed: 20.06.2025).

5. Phiayura, P., and Teerakanok, S. (2023). “A Comprehensive Framework for Migrating to Zero Trust Architecture”, *IEEE Access*, 11, pp. 19487–19511. Available at: https://doi.org/10.1109/ACCESS.2023.3248622.
6. National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture* (NIST Special Publication 800-207).
7. Cybersecurity and Infrastructure Security Agency. *Zero Trust Maturity Model, Version 2.0.* Available at: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (Accessed: 20.06.2025).
8. The National Cyber Security Centre. *Zero trust architecture design principles*. Available at: https://www.ncsc.gov.uk/collection/zero-trust-architecture (Accessed: 20.06.2025).
9. Australian Cyber Security Centre. *Essential Eight*. Available at: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight (Accessed: 20.06.2025).
10. The Law of Ukraine “On information protection in information and communication systems”. 1994. *Vidomosti Verchvnoy Rady Ukrainy*. 31. p. 286.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016) Official Journal L 119, 1-88. http://data.europa.eu/eli/reg/2016/679/oj
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
13. The Law of Ukraine “On Access to Public Information”. 2011. *Vidomosti Verchvnoy Rady Ukrainy*. 32. p. 314.
14. Khudoliy, A. (2019). “Kiberbezbeka: suchasni vyklyky pered Ukrainoyu” [Cybersecurity: modern challenges of Ukraine] *Acta De Historia & Politica: Saeculum XXI*, 1, pp. 138–146. Available at: https://doi.org/10.26693/ahpsxxi2019.01.138
15. Evsyukova, O. (2021). “Osoblyvosti pidgotovky fakhivtsiv u sferi kiberbezpeky: suchasni vyklyky s perspektyvy” [Features of training of specialists in the field of cyber security: current challenges and prospects]. *Derzhavne Upravlinnya: Udoskonalennya ta Rozvytok*. 2. Available at: https://doi.org/10.32702/2307-2156-2021.2.2

DSc, Prof. Bobok I.I., DSc, Prof. Kobozieva A.A.

ZERO TRUST ARCHITECTURE AND PROSPECTS FOR ITS IMPLEMENTATION IN THE GOVERNMENT SECTOR OF UKRAINE

The escalation of cyberattacks as a key component of hybrid warfare poses significant challenges to the security of state information systems. In the context of ongoing military aggression against Ukraine and large-scale attacks targeting critical infrastructure, the traditional perimeter-based security model has proven insufficient under conditions of blurred network boundaries and widespread adoption of cloud technologies and remote access. A promising alternative is the Zero Trust Architecture (ZTA), built on the principles of "never trust, always verify," least privilege access, and continuous monitoring. The aim of this study is to substantiate an adapted ZTA implementation model for Ukrainian government networks, considering national regulatory requirements, limited financial and human resources, and heightened risks during hybrid aggression. The paper provides an overview of leading international frameworks, including NIST SP 800-207, CISA Zero Trust Maturity Model, and NCSC Design Principles, and identifies key barriers to their application in Ukraine. These barriers include outdated infrastructure, regulatory inconsistencies, insufficient personnel expertise, and restricted budgets. The proposed conceptual model incorporates a phased implementation strategy across five layers: identity and access management, dynamic access control, network microsegmentation, data protection, and continuous monitoring with behavioral analytics. The model also integrates federated identity management, multi-factor authentication, contextual risk-based access control, and centralized monitoring via SIEM and SOAR platforms. The expected result is an increased level of cyber resilience in government networks without a significant reduction in usability, ensuring compliance with national cybersecurity standards and readiness for hybrid threats.

Keywords: zero trust, government information systems, cybersecurity, hybrid warfare, identity, microsegmentation, adaptive authentication.