https://doi.org/10.15407/np.77.050
УДК 061:1:342.511](477):004.056]“364”

Людмила Дем’яненко,
кандидат філологічних наук, старший науковий співробітник,
Національна бібліотека України імені В. І. Вернадського
Голосіївський просп., 3, Київ, 03039, Україна
e-mail: demjanenkol@ukr.net
ORCID: https://orcid.org/0000-0002-5160-2736

КОНЦЕПЦІЯ “ZERO TRUST” ЯК СКЛАДОВА АРХІТЕКТУРИ БЕЗПЕКИ ДАНИХ ІНСТИТУТУ ПРЕЗИДЕНТСТВА В УМОВАХ ВІЙНИ

Статтю присвячено дослідженню концепції “Zero Trust” («нульової довіри») як ключового елемента архітектури кібербезпеки інституту президентства в умовах війни. Актуальність теми зумовлена стрімким зростанням кількості кібератак на критичну державну інфраструктуру України з початку повномасштабного вторгнення РФ, що поставило під загрозу функціонування вищих органів державної влади та безперервність здійснення президентських повноважень. У статті розкрито сутність і базові принципи моделі “Zero Trust”, яка передбачає відмову від традиційної периметральної концепції захисту на користь безперервної верифікації кожного контрагента, пристрою та мережевого з’єднання незалежно від їх розташування. Проаналізовано архітектурні складові моделі – мікросегментацію мереж, багатофакторну автентифікацію, принцип найменших привілеїв і безперервний моніторинг – у контексті специфічних вимог до захисту інформаційних систем президентських структур. Досліджено міжнародний досвід імплементації Zero Trust у системах державного управління, зокрема практику США, де відповідна стратегія закріплена на рівні виконавчих директив адміністрації. Проведено порівняльний аналіз з підходами до кіберзахисту президентських інституцій країн НАТО і виявлено спільні організаційно-технічні рішення, прийнятні для адаптації в українських реаліях. Автором обґрунтовано, що впровадження архітектури Zero Trust для інституту президентства є не лише технічним, а й стратегічним рішенням, що безпосередньо впливає на стійкість державного управління в кризових умовах. Сформульовано практичні рекомендації щодо поетапної імплементації моделі з урахуванням обмежень воєнного часу,

наявної інфраструктури та людського фактору як ключової вразливості будь-якої системи кібербезпеки.
Ключові слова: Zero Trust, кібербезпека, інститут президентства, архітектура безпеки даних, критична інфраструктура, війна, державне управління, мікросегментація.

Повномасштабне вторгнення РФ в Україну видозмінило міжсекторальні інформаційні взаємодії та підходи до забезпечення безпеки даних владних структур. Особливо актуальними стали методики Zero Trust – винятково через поєднання воєнних, політичних і цифрових загроз, які одночасно впливають на систему державного управління. Інформаційні системи органів державної влади, зокрема інституту президентства, стали об'єктом постійних кібератак, спроб несанкціонованого доступу, фішингових кампаній, атак на канали зв'язку та інфраструктуру зберігання даних. За таких умов традиційна модель кіберзахисту, побудована на довірі до внутрішнього контуру мережі, уже не забезпечує належного рівня безпеки, оскільки загроза може походити як ззовні, так і зсередини системи. Для України це питання є особливо важливим з огляду на необхідність забезпечення безперервності функціонування вищих органів влади, захисту службової, стратегічної та комунікаційної інформації, а також збереження цілісності управлінських рішень у кризових умовах.

Інститут президентства виконує ключову координаційну функцію в системі національної безпеки, міжнародної дипломатії, оборонного управління та політичної стабільності держави. Відтак будь-яке порушення конфіденційності, цілісності чи доступності даних у цій сфері може мати наслідки не лише технічного, а й безпекового та геополітичного характеру. У контексті цього концепція "Zero Trust" відповідає сучасній логіці захисту в умовах розподіленої, мобільної та змішаної цифрової інфраструктури, адже під час війни значна частина державних процесів здійснюється в умовах підвищеної гнучкості: віддалений доступ, робота через захищені хмарні сервіси, резервування даних, використання різних пристроїв і каналів комунікації. У такому середовищі модель «нікому не довіряй, завжди перевіряй» є найбільш виправданою, оскільки передбачає постійну автентифікацію користувачів, контроль доступу за принципом

найменших привілеїв, сегментацію ресурсів і безперервний моніторинг активності.

Додаткової ваги цій темі надає стратегічний курс України на гармонізацію стандартів кібербезпеки з практиками ЄС і НАТО. Принципи Zero Trust дедалі активніше впроваджуються в державному секторі країн-партнерів, а тому їх дослідження й адаптація до українських реалій є важливими не лише для поточного захисту державних даних, а й для довгострокової інституційної модернізації системи публічного управління. У цьому контексті дослідження Zero Trust як складової архітектури безпеки даних інституту президентства є своєчасним, практично значущим і таким, що має безпосереднє значення для національної стійкості України.

Проблематика впровадження концепції "Zero Trust" у системах кібербезпеки є відносно новою, але динамічно розвивається в сучасній науковій думці. Її становлення пов'язано з переходом від традиційних периметральних моделей захисту до підходів, орієнтованих на безперервну верифікацію доступу та захист даних незалежно від місця розташування суб'єкта чи ресурсу. Серед зарубіжних дослідників ключову роль у формуванні теоретичних засад концепції відіграв Дж. Кіндерваг [1], який уперше сформулював підхід Zero Trust під час роботи в Forrester Research. Його дослідження заклали основу для принципу "never trust, always verify", що став центральним у сучасній кібербезпеці. Подальший розвиток концепції відображено в працях дослідників у сфері системної кібербезпеки, зокрема Б. Лунда та Т. Лі [2], які аналізують Zero Trust як універсальну модель захисту інформаційних середовищ і наголошують на важливості безперервної автентифікації, принципу найменших привілеїв та припущення компрометації системи.

Значний внесок у розвиток методології впровадження Zero Trust зроблено в працях таких дослідників, як З. Кольєр і Дж. Саркіс [3], які визначили критичні фактори успіху та надали оцінку зрілості систем безпеки. Вони пропонують багатовимірну модель впровадження Zero Trust, що включає такі компоненти, як ідентифікація, мережі, дані, аналітика, автоматизація.

Окремий напрям досліджень пов'язаний із систематичними оглядами та узагальненням підходів до Zero Trust Architecture

(ZTA). О. Борхерт, С. Коннелі, С. Мітчел і С. Роуз [4] аналізують її еволюцію, застосування та обмеження в різних галузях, включаючи державне управління й критичну інфраструктуру.

Серед українських дослідників проблематика Zero Trust лише формується, однак уже представлена в працях Г. Головка, І. Тараненка, О. Куща [5], які аналізують переваги моделі над традиційними системами захисту, її застосування в умовах цифрової трансформації, а також виклики імплементації в організаціях.

Враховуючи умови війни, гібридних загроз і постійного кібертиску з боку держави-агресора, виникає потреба в переосмисленні існуючих моделей захисту та переході до більш адаптивних і стійких архітектур. Саме тому обрану наукову проблематику варто більш детально розглянути з точки зору комплексного аналізу можливостей інтеграції принципів Zero Trust у систему забезпечення діяльності інституту президентства з урахуванням українських реалій, наявної інфраструктури та обмежень воєнного часу, що дає змогу не лише заповнити наявну наукову прогалину, а й сформувати практично орієнтовані рекомендації для підвищення кіберстійкості державного управління.

Метою статті є комплексний аналіз концепції "Zero Trust" як складової архітектури кібербезпеки інституту президентства в умовах війни, а також обґрунтування доцільності її впровадження для забезпечення стійкості функціонування вищих органів державної влади та безперервності реалізації президентських повноважень.

Методологічну основу дослідження становить поєднання загальнонаукових і спеціальних методів: аналіз і синтез застосовано для розкриття сутності концепції "Zero Trust" та її ключових компонентів; системний підхід – для розгляду архітектури кібербезпеки інституту президентства як цілісної системи; порівняльний аналіз – для вивчення міжнародного досвіду впровадження відповідних підходів, зокрема в США та країнах НАТО; структурно-функціональний метод – для визначення ролі окремих елементів архітектури (мікросегментації, багатофакторної автентифікації, принципу найменших привілеїв і безперервного моніторингу); узагальнення й моделювання – для формування практичних рекомендацій щодо поетапної імплементації цієї концепції в українських умовах.

Сучасна динаміка розвитку систем кібербезпеки відзначається безпрецедентною швидкістю та мінливістю зміни її компонентів, що обумовлено як прискоренням темпів розвитку нанотехнологій, так і тотально нестабільними процесами в геополітичному полі більшості регіонів. Весь спектр таких видозмін стосується як індивідуальних комунікативних процесів, так і безпеки даних на рівні держави. Так, для України реалії війни позначилися не лише прямими фізичними руйнуваннями, а й новим рівнем кіберзагроз, трансформацією інфраструктури, критичною роллю інституту президентства в мобілізації міжнародної допомоги та забезпечення національної безпеки, вимогами інтеграції й накопичення досвіду протистояння інформаційним і кібератакам РФ. Останні, як показує практика, продовжують спрямовуватися не лише на виведення систем з ладу, а й на викрадення конфіденційних даних, дезінформацію та підрив довіри громадян до органів влади. У контексті цього дедалі більшої популярності в теоретичних пошуках і практичних кейсах державного управління набуває концепція “Zero Trust”, яка була вперше сформульована Дж. Кіндервагом (John Kindervag), який обґрунтував необхідність відмови від традиційної моделі «довіреної мережі» на користь принципу «ніколи не довіряй, завжди перевіряй» (never trust, always verify) [1, с. 3]. Він використав метафору «твердої оболонки з м’якою начинкою» (hard crunchy shell with soft chewy center) для опису вразливості традиційних мережевих архітектур: потужний периметральний захист (firewall, IDS/IPS) створює ілюзію безпеки, тоді як внутрішній трафік практично не контролюється. Відповідно, зловмисник, який подолав периметр або отримав доступ через скомпрометовані облікові дані інсайдера, може вільно переміщатися мережею та отримувати доступ до критичних ресурсів. У контексті цього українські дослідники також зазначають, що «традиційні стратегії кібербезпеки базуються на периметральній обороні, яка передбачає, що все всередині мережі є надійним, тоді як все зовні – ні. Такий підхід мав сенс в епоху, коли організації працювали повністю в локальних середовищах. Однак в епоху хмарних обчислень та віддаленої роботи, ця модель більше не забезпечує достатнього захисту» [5, с. 98]. Тому Zero Trust – це

насамперед архітектура кібербезпеки, розроблена для усунення недоліків захисту на основі периметра.

Швидкий розвиток цієї концепції привів до формування базових принципів, які було систематизовано в спеціальній публікації Національного інституту стандартів і технологій США (NIST SP 800-207):

– усі джерела даних та обчислювальні сервіси вважаються ресурсами: мережа може складатися з різноманітних пристроїв – від серверів до IoT-сенсорів, кожен з них потребує захисту;

– увесь зв'язок є захищеним незалежно від розташування в мережі: запити з «внутрішньої» мережі не є автоматично довіреними, кожне з'єднання має бути автентифіковане й зашифроване;

– доступ до окремих ресурсів надається на основі сесії: автентифікація та авторизація відбуваються для кожного запиту окремо, а довіра до попередніх сесій не переноситься автоматично;

– доступ визначається динамічною політикою: рішення про надання доступу враховує не лише ідентичність користувача, а й стан пристрою, поведінкові патерни, час запиту, геолокацію та інші контекстуальні фактори;

– організація забезпечує моніторинг і вимірювання цілісності й безпекової позиції всіх власних та асоційованих активів: жоден актив не є inherently довіреним;

– автентифікація й авторизація є динамічними та суворо застосовуються перед наданням доступу: це безперервний процес, а не одноразова перевірка;

– організація збирає максимум інформації про поточний стан активів, мережевої інфраструктури, комунікацій і використовує її для покращення безпекової позиції. Моніторинг є не опціональним, а обов'язковим компонентом архітектури [4, с. 6–8].

Дотримання цих принципів і прийняття контекстуальних рішень у подоланні кіберзагроз дали можливість уніфікувати запропонований Дж. Кіндервагом підхід та перетворити Zero Trust з конкретних технічних рішень на те, що Б. Лунд згодом назвав «філософією безпеки та набором архітектурних принципів, які можуть бути реалізовані за допомогою різних технологій і процедур» [2, с. 1521]. Це уточнення стало визначальним щодо сучасних підходів управлінської діяльності, адже передбачало, що впровадження концепції не

може зводитися до встановлення певного програмного забезпечення, воно потребує комплексної трансформації підходів до організації інформаційної безпеки загалом.

Виходячи із цього, уся архітектурна модель Zero Trust включає ряд незмінних компонентів, кожен з яких відіграє специфічну роль у забезпеченні комплексного захисту інформаційних систем, зокрема і у сфері держуправління:

1. Мікросегментація мереж – на відміну від традиційного підходу, де мережа поділяється на кілька великих зон (DMZ, внутрішня мережа, мережа серверів), мікросегментація передбачає створення ізольованих сегментів навколо окремих додатків, сервісів або навіть робочих навантажень. Це дає змогу «обмежити латеральний рух зловмисника в мережі, навіть якщо він отримав початковий доступ до одного із сегментів» [4, с. 14]. У контексті інституту президентства мікросегментація набуває особливого значення, оскільки дає змогу ізолювати найбільш критичні інформаційні ресурси – системи захищеного зв'язку, документообігу, аналітичні бази даних – від менш чутливих компонентів інфраструктури. Навіть у разі компрометації одного сегмента зловмисник не зможе автоматично отримати доступ до інших критичних систем.

2. Багатофакторна автентифікація (MFA) – організації та інститути повинні використовувати автентифікацію й авторизацію перед наданням доступу до будь-якого ресурсу, і ці механізми повинні бути достатньо сильними для рівня чутливості ресурсу. Для систем інституту президентства це означає застосування як мінімум двофакторної автентифікації з використанням апаратних токенів або біометричних даних для доступу до найбільш критичних ресурсів. Дослідниці О. Білик та І. Дорош у своєму дослідженні наголошують, що «впровадження багатофакторної автентифікації для всіх державних службовців, які мають доступ до критичних інформаційних систем, має бути обов'язковою вимогою, а не рекомендацією» [6, с. 11].

3. Принцип найменших привілеїв (Least Privilege) – користувач або система отримує лише той мінімальний набір прав доступу, який необхідний для виконання конкретного завдання. Цей принцип реалізується через механізми рольового (RBAC) та атрибутного

(ABAC) контролю доступу. У контексті Zero Trust він доповнюється концепцією "just-in-time access" – надання підвищених привілеїв лише на обмежений час для виконання конкретної операції з подальшим автоматичним відкликанням.

4. Безперервний моніторинг та аналітика – виявлення аномалій і потенційних загроз у режимі реального часу, зокрема збір та аналіз телеметрії з усіх компонентів інфраструктури органів держуправління (мережевого обладнання, кінцевих точок, додатків, систем ідентифікації). Наприклад, сучасні рішення класу SIEM (Security Information and Event Management) та UEBA (User and Entity Behavior Analytics) дають можливість виявляти підозрілу активність на основі поведінкових патернів. Із цього приводу З. Кольєр і Дж. Саркіс зазначають, що «безперервний моніторинг є не просто технічним інструментом, а фундаментальною зміною парадигми – від реактивного реагування на інциденти до проактивного виявлення та запобігання загрозам» [3, с. 3436].

Сьогодні з точки зору практичного застосування архітектурної моделі Zero Trust США є безумовним лідером у її впровадженні на рівні федерального уряду. У травні 2021 р. на той час Президент США Дж. Байден підписав Виконавчий наказ 14028 «Про покращення кібербезпеки нації» (Executive Order on Improving the Nation's Cybersecurity), який зобов'язав усі федеральні агентства розробити плани переходу до Zero Trust [7]. Цим документом було доручено профільним агентствам, включно з Національним інститутом стандартів і технологій (National Institute of Standards and Technology, NIST), покращувати кібербезпеку держуправління та інших сфер за допомогою різноманітних ініціатив, пов'язаних з безпекою й цілісністю ланцюга постачання програмного забезпечення. До участі було залучено приватний сектор, академічні кола, державні установи й інші організації, а також визначено існуючі та нові стандарти, інструменти, найкращі практики й інші рекомендації для покращення безпеки даних. Ці рекомендації, зокрема, включають: критерії оцінки безпеки програмного забезпечення; критерії оцінки практики безпеки розробників та постачальників; інноваційні інструменти або методи для демонстрації відповідності безпечним практикам. Урядовим органам також було доручено працювати над двома ініціативами

щодо маркування, пов'язаними зі споживчими пристроями Інтернету речей (IoT) та споживчим програмним забезпеченням, з метою заохочення виробників до випуску продуктів, створених з більшим урахуванням ризиків і можливостей кібербезпеки, а покупців – до інформування про них.

На виконання цього Наказу в січні 2022 р. Офіс менеджменту та бюджету (The Office of Management and Budget, OMB) опублікував Меморандум M-22-09 (Memorandum for the heads of executive departments and agencies), який визначив конкретні цілі й терміни впровадження Zero Trust для федеральних агентств. Було передбачено досягнення п'яти стратегічних цілей: централізоване управління ідентичністю, інвентаризація та захист усіх пристроїв, шифрування всього мережевого трафіку, захист додатків як ресурсів, безперервний моніторинг і валідація. Загалом, країни НАТО активно впроваджують принципи Zero Trust у своїх системах державного управління. Агентство НАТО з комунікацій та інформації (The NATO Communications and Information Agency, NCIA) у 2023 р. опублікувало рекомендації щодо застосування Zero Trust для захисту критичної інфраструктури Альянсу, які «передбачають поетапний перехід від периметральної моделі до архітектури нульової довіри» [4, с. 43]. Варто враховувати, що впровадження концептуальних положень Zero Trust в управлінських системах різних країн не завжди відбувається в лінійному форматі, зазвичай це поступальний процес стратегічного значення з різною глибиною імплементування. Для Великої Британії, наприклад, ця концепція стала не просто на рівні тренду, а фундаментальним вектором кібербезпеки всієї системи держуправління. Національний центр кібербезпеки Великої Британії (NCSC) з 2025 р. надає рекомендації щодо побудови і вдосконалення архітектури верифікації шляхом впровадження ZTNA (доступ до мережі з нульовою довірою) замість традиційних VPN, мікросегментації мережі та безперервної автентифікації користувачів і пристроїв.

Серед країн ЄС однією з найбільш кіберстійких вважається Естонія, яка у 2007 р. зазнала однієї з перших загальнонаціональних кібератак у світі – масований напад, що здійснювався з РФ і був спрямований на дестабілізацію критичної інфраструктури, став сигналом тривоги для молодого цифрового суспільства. У відповідь Естонія швидко

прийняла нові закони про кібербезпеку, посилила регулювання та значно інвестувала в підвищення стійкості цифрової інфраструктури на базі підходів Zero Trust. Це був далекоглядний крок, оскільки кібератаки ніколи не припинялися, але країна підтримувала безперебійне надання цифрових послуг. У більшості випадків жителі Естонії не знали, що країна зазнає нападу, при цьому в основі стійкості був X-Road. Створений як ключовий компонент цифрової публічної інфраструктури (DPI) Естонії у 2001 р., X-Road було розроблено для забезпечення безпечного, безперебійного та ефективного обміну даними між державними установами, а також з приватним сектором. Здатність Естонії підтримувати безперебійне надання цифрових послуг, незважаючи на постійні кіберзагрози, не лише забезпечила її власне управління, а й позиціонувала її як модель для інших. Оскільки уряди в усьому світі стикаються з подібними викликами, багато хто звернувся за допомогою до цифрової інфраструктури Естонії. Крім того, із січня 2026 р. набрав чинності Закон про кібербезпеку (Cybersecurity Act), який імплементує європейську директиву NIS2 (Network and Information Security Directive 2) та зобов'язує понад 7 тис. критичних і важливих організацій відповідати жорстким вимогам до безпеки ланцюгів постачання, що робить Zero Trust не просто рекомендацією, а вимогою для бізнесу, який працює з державою.

Досліджуючи імплементацію міжнародних стандартів кібербезпеки, В. Волинець у своєму правовому аналізі зазначає, що «гармонізація українських стандартів кіберзахисту з практиками ЄС і НАТО є не лише політичним зобов'язанням, а й практичною необхідністю для забезпечення сумісності систем у контексті євроатлантичної інтеграції» [8, с. 31]. При цьому впровадження архітектури Zero Trust для інституту президентства України має враховувати специфічні умови воєнного часу, наявну інфраструктуру та організаційні особливості функціонування президентських структур. Також Д. Солодовнік у своєму дослідженні цифрових викликів публічного урядування слушно зазначає, що «цифрова трансформація державного управління в умовах війни відбувається у специфічному контексті: з одного боку, зростає критична залежність від цифрових інструментів, з іншого – суттєво ускладнюються умови забезпечення їх безпеки» [9, с. 112]. До ключових особливостей імплементації можна віднести:

– гібридну інфраструктуру та мобільність. В умовах війни значна частина функцій інституту президентства здійснюється в режимі підвищеної мобільності: віддалені наради, захищений зв'язок з різних локацій, резервування критичних систем. Архітектура Zero Trust має забезпечувати однаковий рівень захисту незалежно від фізичного розташування користувача чи пристрою;

– інтеграцію із системами національної безпеки. Інформаційні системи інституту президентства тісно інтегровані із системами Ради національної безпеки та оборони, Генерального штабу, розвідувальних органів. Упровадження Zero Trust має забезпечувати безшовну й захищену взаємодію між цими системами при збереженні принципу мінімальних привілеїв;

– людський фактор. Він залишається найбільшою вразливістю будь-якої системи кібербезпеки, для інституту президентства це означає необхідність поєднання технічних заходів із систематичним навчанням персоналу, формуванням культури кібергігієни та регулярними тренінгами з реагування на інциденти;

– поетапність упровадження. З урахуванням обмежень воєнного часу – фінансових, кадрових, часових – упровадження Zero Trust має відбуватися поетапно, починаючи з найбільш критичних систем і поступово охоплюючи всю інфраструктуру. Зарубіжні дослідники рекомендують «ітеративний підхід до впровадження Zero Trust, який дає змогу демонструвати швидкі результати та поступово нарощувати зрілість безпекової архітектури» [3, с. 3440].

На сьогодні в Україні поки немає офіційно задекларованого державного органу, який повністю впровадив Zero Trust як цілісну модель, але окремі елементи й принципи активно впроваджуються у ключових кібербезпекових структурах. Серед таких можна назвати: CERT-UA (структурний підрозділ Держспецзв'язку) – відповідає за реагування на кібератаки, працює з постійною верифікацією доступів, моніторингом і сегментацією, застосовує частину принципів Zero Trust (continuous monitoring, threat validation); Державна служба спеціального зв'язку та захисту інформації – координує кіберзахист держави, упроваджує сучасні моделі безпеки для держорганів; Служба безпеки України – відповідає за контррозвідку й кібербезпеку держави, працює з високочутливими

системами, операційно застосовуються контроль доступів, багаторівнева перевірка, принцип "assume breach" та ін.

Важливо наголосити, що в умовах війни українські президентські структури, як і більшість інших держорганів, не можуть запроваджувати Zero Trust як певну брендовану модель, однак мають можливість поступового впровадження відповідних принципів та архітектур, тобто це не завжди одна цілісна система, скоріше, певна стратегія. Тому інститут президентства в Україні де-факто рухається до Zero Trust швидше, ніж в багатьох інших країнах, що обумовлено викликами війни, але скоріше через практики, ніж шляхом розробки актуальних політик.

Висновки. Концепція Zero Trust є адекватною відповіддю на сучасні кіберзагрози, з якими стикається інститут президентства в умовах війни. Традиційна периметральна модель захисту не відповідає реаліям гібридної інфраструктури, зростаючих атак та необхідності забезпечення безперервності державного управління. Тільки поєднання мікросегментації мереж, багатофакторної автентифікації, принципів найменших привілеїв та безперервного моніторингу можуть значно підвищити коефіцієнт безпеки даних. Для інституту президентства України впровадження Zero Trust є не лише технічним, а й стратегічним рішенням, що безпосередньо впливає на стійкість державного управління та національну безпеку. Воно має здійснюватися поетапно, з пріоритетом на найбільш критичні системи та з обов'язковим урахуванням людського фактора.

Перспективи подальших досліджень пов'язані з розробленням детальної методології оцінки зрілості архітектури Zero Trust для державних органів України, а також із вивченням правових аспектів упровадження концепції нульової довіри в контексті чинного законодавства про захист інформації.

Список використаних джерел

1. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. 2010. URL: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (дата звернення: 29.04.2026).

2. Lund B. D., Lee T.-H., Wang Z., Wang T., Mannuru N. R. Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia.* 2024. No. 4. Pp. 1520-1533. https://doi.org/10.3390/encyclopedia4040099

3. Collier Z., Sarkis J. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*. 2021. No. 59 (11). Pp. 3430-3445. https://doi.org/10.1080/00207543.2021.1884311

4. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. *National Institute of Standards and Technology Special Publication 800-207*. 2020. https://doi.org/10.6028/NIST.SP.800-207

5. Головко Г., Тараненко І., Кущ О. Zero Trust: чому традиційні моделі безпеки більше не працюють. *Системи управління, навігації та зв'язку.* 2025. № 2. С. 97–101. https://doi.org/10.26906/SUNZ.2023.2.97-101

6. Білик О., Дорош І. Напрями підвищення безпеки цифрових публічних сервісів за умов воєнних ризиків. *Центральноукраїнський вісник права та публічного управління*. 2026. Вип. 1 (13). С. 7–14. https://doi.org/10.32782/cuj-2026-1-1

7. Improving the Nation's Cybersecurity. 2026. 23.02. URL: https://www.gsa.gov/technology/government-itinitiatives/cybersecurity/executive-order-14028 (дата звернення: 29.04.2026).

8. Волинець В. Правовий аналіз Стратегії кібербезпеки України: окремі актуальні питання. *Публічне право*. 2025. № 2 (58). С. 26–33. https://doi.org/10.32782/2306-9082/2025-58-3

9. Солодовнік Д. Цифрові виклики та інституційні обмеження в системі публічного урядування України. *Публічно-управлінські та цифрові практики.* 2025. № 2 (5). С. 108–116. https://doi.org/10.31673/2786-7412.2025.028587

References

1. Kindervag, J. (2010). *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Retrieved April 4, 2026, from https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

2. Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia*, *4*, 1520-1533. https://doi.org/10.3390/encyclopedia4040099

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

4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *National Institute of Standards and Technology Special Publication 800-207*. https://doi.org/10.6028/NIST.SP.800-207

5. Golovko, G., Taranenko, I., & Kushch, O. (2025). Zero Trust: Why Traditional Security Models no Longer Work. *Control, navigation, and communication systems, 2*, 97-101. https://doi.org/10.26906/SUNZ.2023.2.97-101

6. Bilyk, O., & Dorosh, I. (2026). Directions for improving the security of digital public services in the face of military risks. *Central Ukrainian Journal of Law and Public Administration, 1*(13), 7-14. https://doi.org/10.32782/cuj-2026-1-1

7. Improving the Nation's Cybersecurity. (2026, February 23). U.S. General Services Administration. Retrieved April 4, 2026, from https://www.gsa.gov/technology/government-itinitiatives/cybersecurity/executive-order-14028

8. Volynets, V. (2025). Legal analysis of the Cybersecurity Strategy of Ukraine: some relevant issues. *Public Law, 2*(58), 26-33. https://doi.org/10.32782/2306-9082/2025-58-3

9. Solodovnik, D. (2025). Digital challenges and institutional limitations in the public administration system of Ukraine. *Public Administration and Digital Practices, 2*(5), 108-116. https://doi.org/10.31673/2786-7412.2025.028587

Отримано / Received 01.05.2026
Прийнято / Accepted 24.05.2026
Опубліковано онлайн / Published online 28.07.2026

Liudmyla Demianenko,
PhD (Philol.), Senior Researcher,
V. I. Vernadskyi National Library of Ukraine

3 Holosiivskyi Ave., Kyiv 03039, Ukraine
e-mail: demjanenkol@ukr.net
ORCID: https://orcid.org/0000-0002-5160-2736

THE *ZERO TRUST* CONCEPT AS A COMPONENT OF THE DATA SECURITY ARCHITECTURE OF THE INSTITUTION OF THE PRESIDENCY UNDER WARTIME CONDITIONS

This article examines the *Zero Trust* concept as a key element of the cybersecurity architecture of the institution of the presidency in wartime conditions. The relevance of the topic is driven by the rapid increase in cyberattacks targeting Ukraine's critical state infrastructure since the beginning of the full-scale invasion by the Russian Federation, which has threatened the functioning of the highest bodies of state power and the continuity of presidential authority. The article outlines the essence and core principles of the *Zero Trust* model, which replaces the traditional perimeter-based security approach with continuous verification of every user, device, and network connection, regardless of location. The architectural components of the model - network microsegmentation, multi-factor authentication, the principle of least privilege, and continuous monitoring - are analyzed in the context of the specific security requirements of information systems supporting presidential institutions. The study also explores international experience in implementing *Zero Trust* within public administration systems, particularly in the United States, where the relevant strategy is formalized at the level of executive directives. A comparative analysis is conducted with cybersecurity approaches used in presidential institutions across NATO countries, identifying common organizational and technical solutions that could be adapted to the Ukrainian context. The authors argue that implementing a *Zero Trust* architecture for the institution of the presidency is not only a technical measure but also a strategic decision that directly affects the resilience of public governance in crisis conditions. Practical recommendations are provided for the phased implementation of the model, taking into account wartime constraints, existing infrastructure, and the human factor as a key vulnerability in any cybersecurity system.

Keywords: Zero Trust, cybersecurity, institution of the presidency, data security architecture, critical infrastructure, war, public administration, microsegmentation