УДК 004.056.53:338.49-021.412.1(477) DOI: 10.31673/2412-4338.2025.038702

Трофімов Олександр Сергійович
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0008-5760-7803

ВДОСКОНАЛЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

Анотація. *Стаття присвячена удосконаленню політики захисту інформаційних систем об'єктів критичної інфраструктури (ОКІ) України в умовах цифровізації та гібридної війни. Аргументовано перехід від периметрових моделей до архітектури «повної недовіри» (Zero Trust), що забезпечує контекстну перевірку кожного запиту доступу. Запропоновано інтегровану методику, яка поєднує атрибутивне управління доступом (ABAC), криптографічне управління ключами на базі PKI, порогові схеми розподілу секретів (threshold cryptography), мікросегментацію мереж і безперервний моніторинг. Сформовано загрозо-інформовану модель для ІС критичних секторів (SCADA/ICS, ERP, SIEM/SOC, системи ситуаційної обізнаності, eHealth), що враховує зовнішні та внутрішні сценарії атак. Політику безпеки формалізовано через три компоненти: (1) функцію прийняття рішень доступу на основі атрибутів і контексту; (2) порогове управління секретами для критичних операцій; (3) ризик-скорингову оцінку запитів у реальному часі. Показано відповідність підходу міжнародним і національним вимогам (ISO/IEC 27001:2023, IEC 62443, NIS2, NIST SP 800-207/800-207A, НД ТЗІ), що спрощує аудит і впровадження в українських умовах. Новизна полягає в поєднанні ABAC і механізмів PKI/threshold-криптографії як «криптографічних маркерів довіри» з динамічною мікросегментацією, що мінімізує привілеї, унеможливлює бокове переміщення та підвищує стійкість до компрометації облікових записів і ланцюгів постачання. Практична цінність підтверджена побудовою архітектури політики та сценаріями застосування в енергетиці, транспорті й охороні здоров'я. Результати можуть слугувати основою для секторальних методичних рекомендацій, гармонізації кіберзахисту ОКІ з європейськими стандартами та розроблення дорожньої карти переходу до Zero Trust у державних і корпоративних ІС України.*

Ключові слова: *критична інфраструктура, інформаційна безпека, Zero Trust, криптографічні ключі, розподіл секретів, управління доступом, кіберстійкість.*

Trofimov Olexandr
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0008-5760-7803

IMPROVEMENT OF THE SECURITY POLICY OF INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS OF UKRAINE BASED ON THE ZERO TRUST CONCEPT

Abstract: *The paper addresses the improvement of security policy for information systems of Ukraine's critical infrastructure (CI) amid digitalization and hybrid warfare. It substantiates a shift from perimeter-centric models to the Zero Trust architecture, in which every access request is continuously validated by context. We propose an integrated methodology that combines attribute-based access control (ABAC), PKI-based cryptographic key management, threshold secret sharing, network micro-segmentation, and continuous monitoring. A threat-informed model is developed for representative CI systems (SCADA/ICS, ERP, SIEM/SOC, situational awareness platforms, and eHealth), covering external and insider attack scenarios. The security policy is formalized through three interlinked components: (1) an attribute- and context-driven access decision function; (2) threshold control of secrets for critical operations; and (3) real-time risk scoring of access requests. We show alignment with international and national requirements (ISO/IEC 27001:2023, IEC 62443, NIS2, NIST SP 800-207/800-207A, national TZI rules), which streamlines auditing and practical deployment in Ukrainian environments. The contribution's novelty lies in coupling ABAC with PKI/threshold cryptography as "cryptographic trust markers" together with dynamic micro-segmentation, thereby minimizing privileges, preventing lateral movement, and increasing resilience to account compromise and supply-chain abuse. Practical value is demonstrated by the target policy architecture and application scenarios in energy, transport, and healthcare. The results can underpin governmental and sectoral guidance, harmonize CI cyber defence with European standards, and inform a national roadmap for transitioning to Zero Trust across public and corporate systems in Ukraine.*

Keywords: *critical infrastructure, information security, Zero Trust, cryptographic keys, secret sharing, access management, cyber resilience.*

Вступ

У сучасних умовах цифрової трансформації та гібридної війни проти України об'єкти критичної інфраструктури (ОКІ) дедалі частіше стають ціллю кібератак, що мають потенціал спричинити

масштабні соціально-економічні наслідки. Яскравими прикладами є кібератака на телекомунікаційного оператора «Київстар» у грудні 2023 року [1] та атаки на інформаційні ресурси «Укрзалізниці» у 2025 році [2], які продемонстрували вразливість національних інфраструктурних систем. Це зумовлює нагальну потребу підвищення рівня безпеки інформаційних систем (ІС) ОКІ України [3].

Під інформаційною системою об'єкта критичної інфраструктури розуміється сукупність апаратного та програмного забезпечення, мережевих каналів, баз даних, політик безпеки та користувачів, що забезпечують збирання, обробку, зберігання й передавання інформації для управління критичними технологічними чи адміністративними процесами [5]. Висока залежність державних і приватних підприємств від таких систем робить їх порушення потенційно катастрофічними для енергетики, транспорту, охорони здоров'я, фінансів та інших сфер держави [6].

Традиційні моделі інформаційної безпеки, побудовані на принципі периметрового захисту, дедалі частіше виявляються неефективними [7, 32]. Сучасні загрози характеризуються застосуванням методів соціальної інженерії, APT-атак, зловживанням довірою до внутрішніх користувачів та експлуатацією вразливостей у ланцюгах постачання. У таких умовах концепція «повної недовіри» (Zero Trust), за якою кожен користувач, пристрій чи процес вважається недовіреним до моменту підтвердження автентичності та контекстних атрибутів, розглядається як перспективна альтернатива для побудови ефективної політики безпеки [8, 9, 24].

Нормативно-правове регулювання в Україні вже містить низку вимог щодо кіберзахисту ОКІ. Зокрема, це Закон України «Про критичну інфраструктуру» №1882-IX [11], Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII [12], ДСТУ ISO/IEC 27001:2023 [13], а також національні документи з технічного захисту інформації (НД ТЗІ) [14]. Водночас існує значний розрив між положеннями нормативних актів та практикою впровадження сучасних підходів, що потребує адаптації міжнародних стандартів, зокрема NIST SP 800-207 [15], до українських реалій.

Аналіз літературних даних і постановка проблеми

Аналіз наукових праць і нормативних документів свідчить, що питання захисту інформаційних систем об'єктів критичної інфраструктури України розглядається з кількох ключових позицій. На рівні законодавчого забезпечення визначальне значення мають закони України «Про критичну інфраструктуру» [11] та «Про основні засади забезпечення кібербезпеки України» [12], а також стандарти ISO/IEC 27001 [13] і національні документи з технічного захисту інформації [14]. У міжнародній практиці розроблені універсальні підходи до управління безпекою, зокрема рекомендації IEC 62443 [26], директива ЄС NIS2 [27] і концепція Zero Trust, викладена у NIST SP 800-207 [15].

У наукових дослідженнях значна увага приділяється аналізу вразливостей промислових і корпоративних інформаційних систем. Зокрема, у дослідження компанії WeLiveSecurity [17] розглядаються проблеми захисту SCADA/ICS та ERP-рішень, які інтегрують критично важливі дані й стають об'єктом кібератак. В статті Сальнікова О. Ф., Посмітюх О. І. та Петренко «Ситуаційний центр як ефективний механізм стратегічних комунікацій» [22] досліджується ефективність SIEM/SOC-платформ і систем ситуаційної обізнаності, що відіграють ключову роль у моніторингу та реагуванні на інциденти. Окремо висвітлено питання захисту медичної інформаційної системи eHealth, яка обробляє значні обсяги персональних даних і вимагає підвищеної уваги до конфіденційності та цілісності інформації, про що пишуть Парфонова І., Зінченко О. у «Посилення кібербезпеки у сфері розвитку системи eHealth в Україні» [23].

Попри наявність ґрунтовних досліджень, більшість із них зосереджуються на окремих секторах або окремих технічних аспектах. Традиційна модель периметрової безпеки, яка історично використовувалася в Україні, дедалі частіше виявляється недостатньою для протидії новим викликам — цілеспрямованим атакам на промислові системи, зловживанням довірою внутрішніх користувачів, соціальній інженерії та компрометації ланцюгів постачання, що було детально описано у публікації агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) «Threat Landscape for Industrial Control Systems» [7, 32].

Таким чином, можна констатувати наявність наукової проблеми: існує суттєвий розрив між законодавчими вимогами й практикою захисту інформаційних систем критичної інфраструктури України. Недостатня увага приділяється питанням практичної імплементації концепції Zero Trust, зокрема застосуванню криптографічного управління ключами й механізмів розподілу секретів як основи побудови адаптивної політики інформаційної безпеки. Саме ці аспекти потребують подальшого дослідження та розробки методики, здатної забезпечити стійкість ІС ОКІ до сучасних і майбутніх кіберзагроз.

Мета і задачі дослідження

Метою роботи є розробка та дослідження принципів і методів побудови політики інформаційної безпеки ІС ОКІ України на основі концепції повної недовіри. Для досягнення цієї мети передбачено виконання таких завдань:

– аналіз сучасного стану захисту ІС ОКІ України та існуючих викликів;

– формування моделі загроз з урахуванням ролей користувачів і можливих коаліційних сценаріїв;

– розробка архітектурних і організаційних рішень для вдосконалення політики інформаційної безпеки на основі Zero Trust;

– оцінка перспектив гармонізації національної політики безпеки з міжнародними стандартами та європейськими вимогами.

Результати дослідження

Функціонування об'єктів критичної інфраструктури України спирається на широкий спектр ІС, які забезпечують як технологічні, так і управлінські процеси [9]. У різних секторах використовуються автоматизовані системи диспетчерського управління (АСДУ) [19], платіжні системи Національного банку України та комерційних банків [34], системи управління авіаційним рухом (ATM/ATC) [6], геоінформаційні системи (GIS) [33], урядові мережі спеціального зв'язку [22], а також автоматизовані системи управління технологічними процесами (АСУ ТП) [26]. Кожна з цих категорій має стратегічне значення для забезпечення безпеки держави, адже вихід з ладу таких систем може призвести до суттєвих соціально-економічних наслідків [25].

Разом з тим, для подальшого дослідження обрано лише найбільш типові класи інформаційних систем. До таких віднесено: SCADA/ICS [19], ERP-рішення, SIEM/SOC-платформи, системи ситуаційної обізнаності [22] та медичну інформаційну систему eHealth [23]. Вони представлені в таблиці 1, яка узагальнює ключові характеристики їх застосування в Україні.

Таблиця 1

Типові інформаційні системи об'єктів критичної інфраструктури України

Клас ІС	Сфера застосування	Приклади в Україні	Ключові особливості
SCADA/ICS	Енергетика, транспорт, комунальне господарство	НЕК «Укренерго», оператори обленерго	Диспетчерське керування, збір даних, керування обладнанням у реальному часі [17,19]
ERP	Управління ресурсами підприємств	Укргідроенерго (SAP ERP)	Планування ресурсів, фінансовий облік, інтеграція з технологічними системами [20]
SIEM/SOC	Кіберзахист, моніторинг подій	Урядова СВВ (Держспецзв'язку)	Централізоване виявлення інцидентів, реагування на атаки [21]
Системи ситуаційної обізнаності	Кризове управління, цивільний захист	ДСНС, національна система «112»	Інтеграція даних, координація реагування, диспетчерські центри [22]
eHealth	Охорона здоров'я	Єдина державна електронна система охорони здоров'я	Взаємодія МІС з ЦБД, електронні рецепти, захист персональних даних [23]

Нормативно-правові основи інформаційної безпеки ОКІ

Захист вище згаданих ІС ОКІ України визначається системою законодавчих та нормативних актів. Базові вимоги закріплено в законах «Про критичну інфраструктуру» [11] та «Про основні засади забезпечення кібербезпеки України» [12], які задають принципи стійкості та державної координації. На рівні стандартизації ключову роль відіграє ДСТУ ISO/IEC 27001:2023 [13] як модель СУІБ. Для промислових середовищ доцільно враховувати вимоги IEC 62443 [26], а також рамкові положення директиви ЄС NIS2 [27]. У національній практиці важливими залишаються НД ТЗІ 3.7-003-2023 [14] (порядок створення КСЗІ) та постанова КМУ № 1295 [21] щодо функціонування державної СВВ (система виявлення вразливостей). Додатково постановою КМУ № 518 [28] затверджені Загальні вимоги до кіберзахисту ОКІ, що забезпечує зв'язок між правовими нормами та впровадженням технічних і організаційних заходів.

Нормативна база охоплює як загальні принципи, так і галузеві вимоги до ІС критичної інфраструктури, поступово гармонізуючись з міжнародними стандартами. Однак низка положень залишається декларативною, що актуалізує необхідність їх практичної реалізації, зокрема через концепцію Zero Trust.

Типові загрози та виклики для захисту ІС ОКІ

На сьогоднішній день ІС ОКІ України функціонують в умовах постійного зростання кількості та складності кібератак, що формує комплекс специфічних загроз і викликів. Одним із ключових чинників ризику є спрямованість атак на промислові системи керування, про що свідчать відомі інциденти із застосуванням шкідливого ПЗ «Industroyer2» проти енергетичного сектору [17]. Цілеспрямовані атаки на SCADA/ICS демонструють здатність порушувати технологічні процеси, що безпосередньо впливає на безперервність критичних послуг.

Не менш актуальними є загрози для ERP-систем, які інтегрують фінансові та виробничі дані. Їх компрометація може призвести до витоку комерційно чутливої інформації або порушення бізнес-процесів. Водночас ERP часто інтегровані з іншими інформаційними платформами, що створює додаткові ризики поширення атаки по всьому інформаційному середовищу [20].

У сфері моніторингу та реагування особливим викликом залишається недостатня ефективність SIEM/SOC-рішень через обмеженість ресурсів, кадровий дефіцит та потребу в інтеграції великої кількості різнорідних джерел подій. Попри запуск державної СВВ [21], залишається проблема низької швидкості обробки даних і недостатньої автоматизації реагування.

Системи ситуаційної обізнаності та кризового управління, включаючи «112», стикаються з ризиками відмов у доступності через DDoS-атаки, а також із загрозами компрометації каналів зв'язку під час надзвичайних ситуацій [22]. Уразливість таких систем становить критичний фактор, адже їхнє порушення унеможливлює координацію дій служб реагування.

Особливої уваги потребує захист медичної інформаційної системи eHealth, оскільки вона містить значні обсяги персональних і медичних даних громадян. Основними ризиками тут є несанкціонований доступ, витік конфіденційної інформації та можливість маніпуляції даними, що прямо впливає на довіру населення до державних цифрових послуг як у сфері охорони здоров'я [23], так і загалом.

Крім технічних загроз, характерним викликом для всіх ІС ОКІ є внутрішні ризики: помилки або недостатня кваліфікованість персоналу, зловживання повноваженнями або навмисні дії інсайдерів. В умовах кадрового дефіциту у сфері кібербезпеки такі ризики посилюються. Додатковим чинником є застаріле обладнання та програмне забезпечення, яке не завжди відповідає сучасним вимогам безпеки, а також складність інтеграції нових рішень у вже існуючу інфраструктуру.

Формування моделі загроз для ІС ОКІ на основі концепції Zero Trust

Узагальнення сучасних загроз та стану захисту інформаційних систем ОКІ показало обмежену дієвість традиційних моделей безпеки. Це зумовлює потребу у пошуку нових підходів, здатних забезпечити стійкість у динамічному середовищі атак. Традиційні підходи до захисту ІС ОКІ базувалися на концепції периметрової безпеки, яка передбачає наявність чіткої межі між «зовнішнім» та «внутрішнім» середовищем. У межах такої моделі користувачі та процеси, що перебувають усередині периметру, здебільшого вважалися довіреними. Однак сучасна практика доводить обмеженість цього підходу, оскільки основні загрози надходять як із зовнішнього середовища, так і зсередини організації [17]. Крім того, значна кількість атак реалізується через компрометацію облікових записів, використання вразливостей обладнання або зловживання довірою до підрядників та інсайдерів.

У відповідь на ці виклики в міжнародній практиці сформувалася концепція «повної недовіри» (Zero Trust), яка виходить з принципу «нікому не довіряй — завжди перевіряй» [8, 15]. Відповідно до цього підходу, жоден суб'єкт чи процес не вважається безпечним апріорі, а кожен запит на доступ підлягає перевірці незалежно від його походження. Таким чином, доступ до ресурсів визначається не лише належністю користувача до певної мережі чи сегменту, але й додатковими факторами — автентифікацією, станом пристрою, рівнем привілеїв, чутливістю запитуваних даних. Ключовими складовими Zero Trust є:

- мінімізація довіри (надання лише необхідних у конкретний момент повноважень);
- багаторівнева автентифікація та безперервна верифікація;
- мікросегментація мережі, що унеможливлює неконтрольоване переміщення між сегментами;
- контекстно-орієнтоване управління доступом на основі атрибутів користувача, пристрою, операції та ресурсу;
- постійний моніторинг і аналіз поведінки для виявлення аномалій.

Застосування цих принципів дозволяє розглядати захист ІС як динамічний процес, у якому рівень довіри формується ситуативно й переглядається на основі контекстних даних у режимі реального часу. Такий підхід закладає основу для побудови адаптивної політики безпеки, здатної реагувати на динаміку загроз та забезпечувати стійкість критичних секторів навіть за умов цілеспрямованих атак. Водночас практична реалізація цих принципів вимагає надійних технічних засобів підтвердження

довіри, серед яких ключову роль відіграють механізми управління криптографічними ключами. Саме вони становлять базовий елемент автентифікації, авторизації та захисту даних, забезпечуючи функціонування концепції «повної недовіри», де доступ до ресурсів формується виключно на основі підтверджених атрибутів користувача та захищених каналів обміну [13].

У практиці кіберзахисту ключову роль відіграє інфраструктура відкритих ключів (PKI), яка забезпечує створення, поширення, відкликання та оновлення сертифікатів цифрових ключів. Для інформаційних систем ОКІ використання PKI дозволяє:

- забезпечити унікальну ідентифікацію кожного користувача та пристрою;
- гарантувати цілісність та автентичність даних під час їх обміну;
- реалізувати багаторівневу автентифікацію, у тому числі із застосуванням апаратних токенів, смарт-карток чи модулів HSM;
- організувати динамічне управління доступом, коли ключі можуть мати обмежений термін дії або прив'язку до конкретного контексту (час, місце, тип операції).

У контексті розподілу секретів особливе значення мають механізми багатостороннього управління ключами (threshold cryptography), які передбачають розподіл секретного ключа на декілька частин між незалежними сторонами. Це дозволяє знизити ризики компрометації, адже відновлення повного ключа можливе лише за умови кооперації визначеної кількості учасників [26, 27]. У випадку ОКІ такий підхід може застосовуватись для критично важливих операцій — наприклад, зміни конфігурацій SCADA-систем чи підпису транзакцій у фінансових розрахунках.

Важливим аспектом є також захист процесів управління ключами: безпечне зберігання в HSM-модулях, регулярна ротація, використання протоколів на кшталт TLS 1.3 із сучасними алгоритмами шифрування, а також дотримання національних стандартів криптографічного захисту інформації (ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002) [14, 28]. Поєднання таких технічних заходів із організаційними процедурами (розмежування ролей, багаторівневе погодження доступу) забезпечує відповідність як міжнародним стандартам, так і національним нормативним вимогам.

Таким чином, ефективне управління криптографічними ключами виступає основою для практичної реалізації концепції Zero Trust в інформаційних системах критичної інфраструктури. Воно дозволяє поєднати механізми ідентифікації, автентифікації та контролю доступу в єдину систему, що забезпечує стійкість до зовнішніх і внутрішніх загроз та створює передумови для побудови захищеного механізму розподілу секретів.

Побудова формалізованої моделі загроз

Врахування описаних у розділі 2 загроз дозволяє визначити необхідність впровадження методики, що поєднує принципи Zero Trust з механізмами управління криптографічними ключами. Її сутність полягає у створенні багаторівневої системи розмежування доступу, в якій кожен користувач та процес вважається потенційно недовіреним, а всі операції з інформаційними ресурсами підлягають криптографічному підтвердженню [4].

Методика включає такі положення:

1. Атрибутивне управління доступом. Доступ до ресурсів визначається не лише роллю користувача, але й контекстними атрибутами (місце, час, тип операції, рівень критичності ресурсу). Це забезпечує реалізацію принципу «мінімально необхідних повноважень» у динамічному режимі [15].
2. Використання криптографічних ключів як маркерів довіри. Кожен користувач і пристрій отримує унікальний криптографічний ключ, виданий інфраструктурою PKI. Будь-яка операція — від автентифікації до зміни конфігурації системи — підтверджується підписом ключа, що унеможливлює виконання дій анонімними чи неавторизованими суб'єктами [29].
3. Механізм розподілу секретів. Для виконання критично важливих операцій (наприклад, відновлення SCADA після аварії чи підпису фінансових транзакцій) застосовується threshold cryptography, яка потребує кооперації кількох уповноважених осіб. Це знижує ризик зловживань з боку інсайдерів і робить неможливим одноосібне прийняття рішень у критичних сценаріях [29, 30].
4. Мікросегментація та контроль трафіку. Доступ до сегментів мережі SCADA, ERP або eHealth дозволяється лише після підтвердження криптографічного маркера довіри. Переміщення між сегментами супроводжується повторною перевіркою ключів і контексту.
5. Постійний моніторинг і переоцінка довіри. Центральна система моніторингу (SOC/СВВ) здійснює збір журналів автентифікації, використання ключів та поведінкових характеристик користувачів. У разі виявлення аномалій (підозрілих транзакцій, масових звернень до даних, зміни поведінки користувача) застосовуються додаткові перевірки, включно з блокуванням ключів.

У відповідності до рекомендацій NIST SP 800-207A [31], побудова моделі загроз у межах Zero Trust повинна бути «загрозо-інформованою» (threat-informed), тобто відштовхуватися від конкретних сценаріїв атак, найбільш імовірних для цільового середовища. Це дозволяє не лише формувати універсальні політики доступу, але й адаптувати їх до динаміки атак, що підтверджується сучасними дослідженнями ENISA [32]. На основі цих положень формується модель загроз, узагальнено подана на рисунку 1.

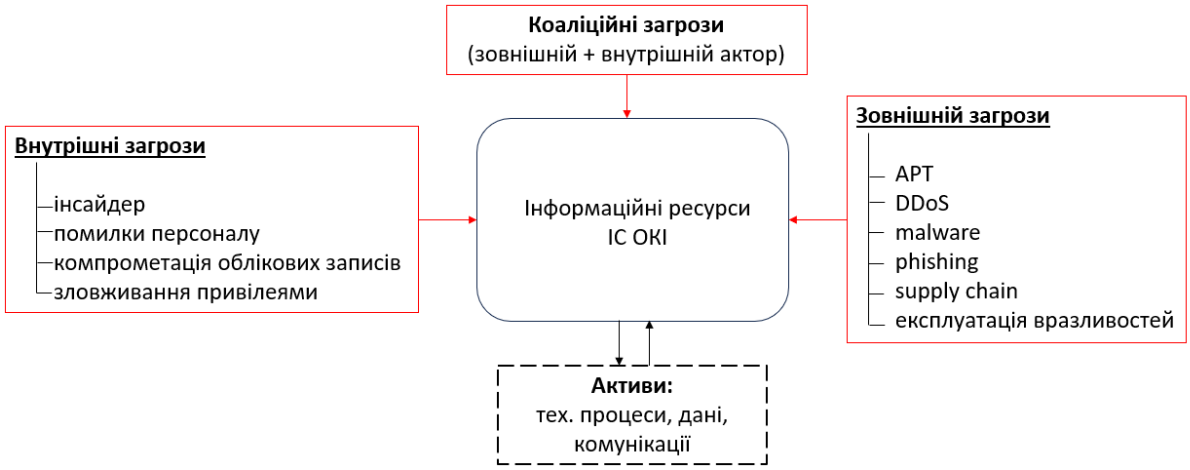

Рис. 1. Модель загроз ІС ОКІ України на основі концепції повної недовіри

У центрі моделі розташовані ключові інформаційні системи ОКІ (SCADA/ICS, ERP, SIEM/SOC, системи ситуаційної обізнаності, eHealth). На них спрямовані три групи загроз: зовнішні (APT, DDoS, фішинг, шкідливе ПЗ), внутрішні (інсайдери, помилки персоналу, компрометація облікових записів) та коаліційні (зовнішній зловмисник у взаємодії з внутрішнім). Ціллю атак є активи — технологічні процеси, дані та комунікації.

Вдосконалення політики інформаційної безпеки ОКІ на основі концепції Zero Trust

Описані загрози та особливості функціонування ІС ОКІ України демонструють, що існуюча політика інформаційної безпеки носить переважно декларативний характер. Законодавча база задає загальні принципи, проте практична імплементація значною мірою залишається фрагментарною та недостатньо узгодженою між секторами [11, 12]. Серед основних проблем можна виокремити:

- обмежене застосування ризик-орієнтованого підходу, коли безпекові рішення приймаються не виходячи з реальної оцінки загроз, а здебільшого на основі формального дотримання вимог;
- недостатню інтеграцію державних і корпоративних політик, що призводить до різнорівневої зрілості захисту у різних галузях;
- відсутність чітких механізмів практичного застосування нормативних актів, у тому числі процедур адаптації до динамічного середовища атак;
- обмежений рівень автоматизації моніторингу та реагування, що зумовлює затримки у локалізації та нейтралізації інцидентів.

Такі недоліки створюють суттєві ризики для забезпечення стійкості ОКІ, особливо з огляду на зростаючу кількість цілеспрямованих атак на енергетичний, транспортний та медичний сектори [17, 23]. Традиційна модель периметрової безпеки, яка історично використовувалася в Україні, не відповідає реаліям сучасного середовища, адже не враховує внутрішні загрози та коаліційні атаки, що комбінують зовнішній та внутрішній вплив.

У зв’язку з цим одним із ключових завдань удосконалення політики інформаційної безпеки є перехід від статичних декларацій до динамічної моделі управління ризиками, що базується на принципах Zero Trust. Такий підхід дозволить:

- розглядати кожного користувача, процес і пристрій як потенційно небезпечний елемент до моменту перевірки;
- здійснювати постійну переоцінку рівня довіри з урахуванням контексту;
- забезпечити прозорість доступу до критичних ресурсів через криптографічні механізми автентифікації й розподілу секретів.

Впровадження нової політики інформаційної безпеки на базі концепції Zero Trust формує підґрунтя для створення цілісної та уніфікованої системи захисту, здатної адаптуватися до динамічного характеру сучасних кіберзагроз і підвищувати рівень стійкості об’єктів критичної інфраструктури навіть в умовах кризових ситуацій, та передбачає впровадження низки ключових компонентів, що

забезпечують цілісність, конфіденційність і доступність інформаційних ресурсів. Кожен з них має конкретну функціональність та спрямований на мінімізацію впливу як зовнішніх, так і внутрішніх загроз. Визначені компоненти становлять базову архітектуру удосконаленої політики безпеки, яка забезпечує комплексний підхід до захисту критичних інформаційних систем України, орієнтований на сучасні виклики та міжнародні стандарти.

Мінімізація довіри та багаторівнева автентифікація

В основі Zero Trust лежить принцип надання лише мінімально необхідних повноважень. Це означає, що кожному користувачу та пристрою визначаються чітко обмежені права доступу, релевантні виключно до виконуваних завдань. Обов'язковим елементом є багатофакторна автентифікація, яка значно знижує ризики компрометації облікових записів у результаті фішингових атак чи підбору паролів [15].

Криптографічне управління ключами і розподіл секретів

Безпекова модель Zero Trust базується на гарантії криптографічної автентичності всіх учасників процесу. У цьому контексті важливим компонентом є PKI, яка забезпечує генерацію, розповсюдження та відкликання ключів. Для операцій із високим рівнем критичності доцільним є застосування threshold cryptography, що дозволяє здійснювати дії (наприклад, зміни у SCADA чи ERP) лише за участі кількох уповноважених осіб [29, 30].

Мікросегментація мереж і контроль трафіку

Системи ОКІ зазвичай включають як IT-, так і OT-складові (технології оперативного управління). Їх об'єднання без належної ізоляції створює високі ризики поширення атак. Мікросегментація мереж передбачає створення ізольованих сегментів, доступ до яких надається виключно після перевірки криптографічних атрибутів довіри. Такий підхід унеможливлює «бокове переміщення» зловмисників у разі компрометації одного вузла [26].

Атрибутивне управління доступом (ABAC)

Модель ABAC дозволяє визначати доступ не лише за роллю користувача, а й за додатковими атрибутами: часом доби, географічним розташуванням, типом пристрою, рівнем чутливості даних. Це забезпечує гнучкість і динамічність управління доступом, що особливо актуально для розподілених систем ОКІ [31].

Моніторинг, реагування та автоматизація

Розбудова SOC та інтеграція його з державною СВВ [21] створює умови для централізованого моніторингу, виявлення аномалій і реагування на інциденти. Для скорочення часу між виявленням та ліквідацією загроз застосовуються автоматизовані системи кореляції подій і блокування шкідливих дій у реальному часі.

Аудит і актуалізація політик

Політика Zero Trust передбачає постійне вдосконалення. Це досягається шляхом регулярних перевірок системи захисту, оновлення політик доступу, тестування механізмів резервування та аварійного відновлення. Особливу роль відіграє аудит процесів управління ключами та автентифікації, оскільки їх компрометація становить найвищу загрозу для всієї системи [32].

Таким чином, визначені компоненти становлять базову архітектуру удосконаленої політики безпеки, яка забезпечує комплексний підхід до захисту критичних інформаційних систем України, орієнтований на сучасні виклики та міжнародні стандарти. Узагальнене подання архітектури політики Zero Trust для ОКІ наведено на рисунку 2.

Схема відображає три рівні: користувачі та пристрої, рівень контролю доступу на основі принципів Zero Trust та рівень захищених інформаційних систем. На середньому рівні представлено ключові компоненти: багатофакторну автентифікацію, PKI та управління ключами, порогові схеми розподілу секретів, атрибутивний контроль доступу, мікросегментацію та систему моніторингу з реагуванням. Саме цей рівень виступає ядром політики безпеки, забезпечуючи постійну перевірку довіри й блокування несанкціонованих дій. Нижній рівень ілюструє захищені системи ОКІ — SCADA/ICS, ERP, SIEM/SOC, ситуаційні центри та eHealth, до яких доступ надається лише після перевірки всіх умов політики.

В свою чергу, ефективність політики інформаційної безпеки безпосередньо залежить від її відповідності чинній законодавчій та нормативній базі. У випадку України важливо не лише інтегрувати принципи Zero Trust у внутрішні процеси об'єктів критичної інфраструктури, а й узгодити їх із національними та міжнародними вимогами.

Фундаментальну основу задають закони України «Про критичну інфраструктуру» [11] та «Про основні засади забезпечення кібербезпеки України» [12], які визначають базові категорії ОКІ, відповідальність суб'єктів та загальні принципи кіберзахисту. У практичній площині ключову роль

відіграють нормативні документи з технічного захисту інформації. Зокрема, НД ТЗІ 3.7-003-2023 [14] визначає порядок створення комплексних систем захисту інформації, постанова КМУ № 1295 [21] регламентує функціонування Системи виявлення вразливостей і реагування на інциденти, а постанова КМУ № 518 [28] встановлює загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.

Важливим завданням є гармонізація національної політики з міжнародними нормами. У першу чергу — із ДСТУ ISO/IEC 27001:2023 [13], що відповідає міжнародному стандарту ISO/IEC 27001:2022, а також зі стандартами серії IEC 62443 [26], які орієнтовані на захист промислових систем управління. Директива ЄС NIS2 [27] визначає загальноєвропейські вимоги до кіберстійкості критичних секторів, а рекомендації NIST SP 800-207A [31] конкретизують практичні аспекти побудови Zero Trust з урахуванням моделювання загроз. Додатковим джерелом практик виступають аналітичні матеріали ENISA, включно з NIS360 – 2024 [32], які відображають сучасний стан кіберзахисту в європейських країнах.

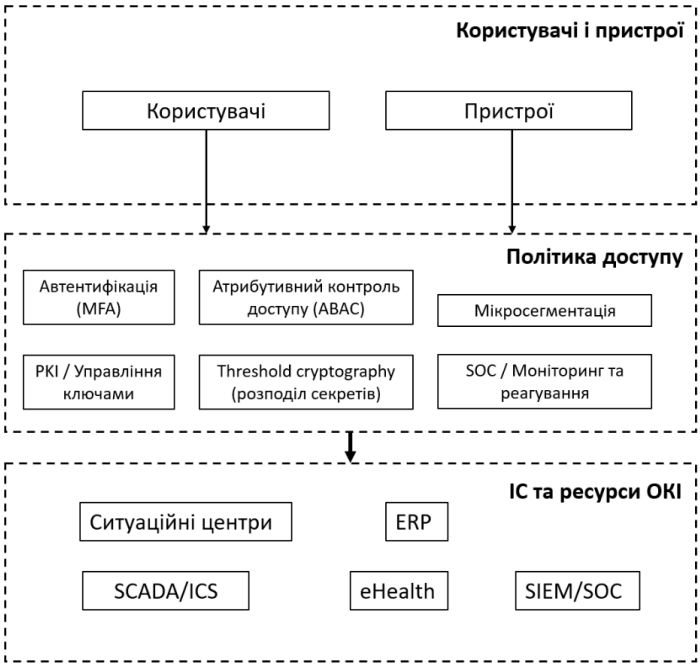

Рис. 2. Архітектура політики Zero Trust для ІС ОКІ України

Попри наявність зазначених документів, в Україні досі бракує практичних методичних рекомендацій щодо впровадження Zero Trust у різних секторах критичної інфраструктури. Технологічні особливості енергетики, транспорту чи охорони здоров'я потребують специфічних сценаріїв реалізації політики доступу, контролю трафіку та управління ключами. Тому доцільним є розроблення державних керівних принципів, які б містили:

- секторальні вимоги до побудови архітектури Zero Trust;
- типові моделі доступу та приклади застосування атрибутивного контролю;
- алгоритми взаємодії з державною СВВ для моніторингу та реагування.

Таким чином, адаптацію слід здійснювати шляхом поєднання положень національного законодавства, міжнародних стандартів і практичних методичних матеріалів. Це дозволить створити єдину систему, яка не лише відповідатиме внутрішнім вимогам, але й забезпечуватиме сумісність із європейським середовищем кібербезпеки.

Задля посилення теоретичного підґрунтя запропонованих підходів доцільним є формалізоване представлення політики інформаційної безпеки ОКІ у рамках концепції Zero Trust. Зокрема, ключові аспекти цієї політики можуть бути описані через математичні моделі, які відображають правила доступу, управління ключами та оцінку ризиків.

Модель функції доступу

Право доступу до ресурсу визначається функцією:

$$Access(U, R, C) \rightarrow \{Allow, Deny\} \quad (1)$$

де A_i - атрибут (роль, час доступу, геолокація, тип пристрою, чутливість даних). Доступ дозволяється лише за умови одночасного виконання всіх правил політики:

$$C = \{A_1, A_2, \dots A_n\} \quad (2)$$

де $U -$ користувач, R – ресурс, C - контекст. Контекст включає множину атрибутів:

$$Access(U, R, C) = Allow \iff \forall A_i \in C : Policy(A_i) = True \quad (3)$$

Модель розподілу секретів

Важливою складовою Zero Trust є контроль критичних операцій, де недопустимим є одноосібний доступ. Для формалізації цього принципу застосовується схема порогового розподілу (threshold cryptography). Секрет S (наприклад, ключ доступу до SCADA) ділиться на n частин:

$$S \to \{s_1, s_2, \dots s_n\} \quad (4)$$

Відновлення секрету можливе лише за умови кооперації щонайменше q учасників ($q \leq n$):

$$S = f(s_{i_1}, s_{i_2}, \dots, s_{i_q}) \quad (5)$$

де f – функція інтерполяції (наприклад, поліном Шаміра). Такий підхід унеможливлює одноосібний доступ до критичних операцій [29, 30].

Модель ризику доступу

Оскільки доступ залежить не лише від автентифікації, а й від умов його здійснення, політика Zero Trust враховує фактори ризику. Для цього кожному запиту може присвоюватися оцінка ризику:

$$Risk(U, R, C) = \sum_{i=1}^{n} w_i \cdot v_i \quad (6)$$

де w_i – ваговий коефіцієнт атрибуту, v_i – значення ризику, пов'язане з атрибутом (наприклад, доступ у неробочий час або з незареєстрованого пристрою). Доступ дозволяється лише у разі, якщо значення ризику не перевищує встановленого порога:

$$Access(U, R, C) = Allow \Leftrightarrow Risk(U, R, C) \leq T \quad (7)$$

Інтегрована модель

Усі наведені вище складові можуть бути поєднані в інтегрованій формалізованій моделі політики Zero Trust, яка описується трьома взаємопов'язаними рівнями:

1. Функція доступу на основі атрибутів (ABAC).
2. Порогове управління секретами для критичних операцій.
3. Оцінка ризику доступу в режимі реального часу.

Запропонована модель поєднує математичну строгість із практичними механізмами безпеки, забезпечуючи можливість формалізованого аудиту та впровадження у системах критичної інфраструктури. Вона не лише демонструє теоретичну реалізованість концепції Zero Trust, але й створює підґрунтя для її практичного застосування в українських умовах. З огляду на актуальні виклики, пов'язані з кібератаками на критичні сектори, впровадження запропонованої політики може стати одним із чинників підвищення національної кіберстійкості та забезпечення відповідності України європейським стандартам кібербезпеки.

Висновки і перспективи подальших досліджень

У результаті проведеного дослідження узагальнено сучасний стан захисту інформаційних систем об'єктів критичної інфраструктури України та обґрунтовано доцільність переходу від традиційних моделей периметрового захисту до концепції Zero Trust. Запропоновано комплексне вдосконалення політики інформаційної безпеки ОКІ, що включає: управління криптографічними ключами як базовий механізм автентифікації та авторизації, формалізоване подання політики у вигляді математичних моделей, а також інтеграцію підходів моніторингу й оцінки ризиків доступу. Зроблено акцент на

необхідності поєднання технологічних і нормативно-правових рішень для створення єдиного захищеного середовища.

Практичне значення результатів полягає у можливості використання запропонованих підходів як основи для державних методичних рекомендацій з кіберзахисту ОКІ, що забезпечить відповідності європейським стандартам кібербезпеки та сприятиме зміцненню національної стійкості до кіберзагроз.

Подальші дослідження доцільно зосередити на розробленні алгоритмів динамічного управління довірою в умовах багатосегментних систем, інтеграції Zero Trust із системами виявлення аномалій на основі штучного інтелекту, а також на формуванні стандартів державного рівня для оцінки ефективності політик безпеки. Перспективним напрямом є також дослідження взаємодії концепції Zero Trust з існуючими міжнародними стандартами (ISO/IEC 27001, NIST SP 800-207A) з метою гармонізації національної нормативної бази із глобальними вимогами.

Список використаної літератури

1. Команда реагування на комп'ютерні надзвичайні події України (CERT-UA) (2023). Кібератака на «Київстар». Звіт Держспецзв'язку — Режим доступу: https://cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar

2. Міжнародне агентство новин «Reuters» (2025). Ukraine's railways restore half of IT services after cyber attack — Режим доступу: https://www.reuters.com/world/europe/ukraines-railways-restore-half-it-services-hit-by-cyber-attack-so-far-2025-04-09/

3. Ільєнко А., Телющенко В., Дубчак О. (2023) Сучасні кіберзагрози критичної інфраструктури України та світу. Кібербезпека: освіта, наука, техніка, 3(27), с. 150–164. DOI: https://doi.org/10.28925/2663-4023.2023.27.719

4. Сиротинський Р., Тишик І., Кочан О., Соколов В., Складанний П. (2024) Методологія аналізу мережевої інфраструктури в рамках переходу до архітектури нульової довіри Cyber Security and Data Protection, vol. 3800, 97–105.

5. Закон України «Про інформацію» №2657-XII від 02.10.1992 (зі змінами) — Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

6. Звіт Center for Security Studies при ETH Zürich (2024). Аналіз стійкісті критичної інфраструктури України в умовах кібератак та військової агресії — Режим доступу: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RR-Report-2024-Critical-Infrastructure-Resilience.pdf

7. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) (2021). Threat Landscape for Industrial Control Systems — Режим доступу: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

8. Kindervag, J. (2010). Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research. — Режим доступу: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

9. Ворохоб М., Киричок Р., Яскевич В., Добришин Ю., Сидоренко С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

10. Крючкова Л., Складанний П., Ворохоб М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Кібербезпека: освіта, наука, техніка, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

11. Закон України «Про критичну інфраструктуру» № 1882-IX (2021). — Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20

12. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (2017). — Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

13. Стандарт ДСТУ ISO/IEC 27001:2023. — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page?id_doc=103359

14. Нормативний документ НД ТЗІ 3.7-003-2023. — Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024

15. NIST (2020). Zero Trust Architecture (SP 800-207). — Режим доступу: https://doi.org/10.6028/NIST.SP.800-207

16. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Бороденко Д. В. (2024). Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Вісник ЛДУБЖД, 30, 67–77. https://doi.org/10.32447/20784643.30.2024.07

17. ESET & CERT-UA. (2022). Industroyer2: Industroyer reloaded. — Режим доступу: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

18. Цехмейстер Р., Платоненко А., Ворохоб М., Черевик В., Семеняка С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. Кібербезпека: освіта, наука, техніка, 3(27), 63–71. https://doi.org/10.28925/2663-4023.2025.27.703

19. Національна енергетична компанія «Укренерго» (2020). УКРЕНЕРГО та SIEMENS модернізують систему диспетчерського керування SCADA. — Режим доступу: https://ua.energy/general-news/ukrenergo-and-siemens-are-upgrading-scada-dispatch-control-system-2/

20. Черненко Ю., Бедрій Д., Гайдаєнко О., Меліксетов О. (2025). Зниження операційних ризиків у критичній інфраструктурі шляхом інтеграції ERP-BPMS: багатоаспектне дослідження. Технологічний аудит та резерви виробництва, 3–4(83), 53–63. https://doi.org/10.15587/2706-5448.2025.330660

21. Постанова КМУ № 1295 від 23.12.2020 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки». https://zakon.rada.gov.ua/go/1295-2020-%D0%BF

22. Сальнікова О. Ф., Посмітюх О. І. та Петренко, М. І. (2021). Ситуаційний центр як ефективний механізм стратегічних комунікацій. Інвестиції: практика та досвід, 2021(17), 62–66. DOI: 10.32702/2306-6814.2021.17.62 http://www.investplan.com.ua/?op=1&z=7584

23. Парфонова І., Зінченко О. (2024). Посилення кібербезпеки у сфері розвитку системи eHealth в Україні. Медичні перспективи. 29(4), 247–256. https://www.researchgate.net/publication/387494749_Cybersecurity_enhancement_in_the_field_of_eHealth_system_development_in_Ukraine

24. Складанний П., Трофімов О., Корнієць В., Ворохоб М., Опришко Т. (2023) Удосконалення політики безпеки системи дистанційного навчання на основі концепції Zero Trust CPITS 2023: Workshop on Cybersecurity Provision in Information and Telecommunication Systems. с. 97-106. ISSN 1613-0073

25. Бржевська З., Киричок Р., Платоненко А., Гулак Г. (2022). Оцінка передумов формування методики оцінки достовірності інформації. Кібербезпека: освіта, наука, техніка, 3(15), 164–174. https://doi.org/10.28925/2663-4023.2022.15.164174

26. Стандарт ДСТУ EN IEC 62443-3-2:2022 — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=107712

27. Директива ЄС «Про заходи щодо забезпечення високого загального рівня кібербезпеки на всій території Союзу». (2022). — Режим доступу: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

28. Постанова Кабінету Міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». — Режим доступу: https://zakon.rada.gov.ua/go/518-2019-%D0%BF

29. Барбараці М., Шмід Н., Альпос О., Сенн М., Кашин К. (2025) Thetacrypt: розподілений сервіс для порогової криптографії. arXiv preprint. https://doi.org/10.48550/arXiv.2502.03247

30. Гулак Г., Мухачов В., Хорошко Ю., Яремчук Є. (2011) Криптографічні протоколи. Основи криптографічного захисту інформації. с. 162-176. ISBN 978-966-641-430-7

31. NIST. (2023). Zero Trust Architecture: A Threat-Informed Approach (SP 800-207A). National Institute of Standards and Technology. — Режим доступу: https://doi.org/10.6028/NIST.SP.800-207A

32. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) (2024). NIS360 – 2024. European Union Agency for Cybersecurity. — Режим доступу: https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf

33. Компанія Esri. (2024). Відбудова української інфраструктури. — Режим доступу: https://www.esri.com/about/newsroom/arcuser/ukraine-hub/

34. Національний банк України. (2023). Система електронних платежів (СЕП). — Режим доступу: https://bank.gov.ua/ua/payments/sep