

Viktor Stepanov

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ZERO TRUST ARCHITECTURE FOR PROTECTING THE DIGITAL INFRASTRUCTURE OF A HIGHER EDUCATION INSTITUTION

Abstract. The paper examines the application of zero trust architecture to the digital infrastructure of a higher education institution where local information systems, cloud services, personal devices, and remote access coexist. The traditional assumption that an internal network location is sufficient for trust is rejected. A staged implementation model is proposed: asset inventory, stronger identity assurance, device posture control, least-privilege access, segmentation, centralized logging, and automated response. Zero trust is treated not as a standalone product but as a policy and architecture principle requiring continuous verification of user identity, device state, context, and resource criticality.

Keywords: zero trust, cybersecurity, identity, access control, higher education institution, digital infrastructure.

Віктор Степанов

Київський національний університет імені Тараса Шевченка, Київ, Україна

АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ ДЛЯ ЗАХИСТУ ЦИФРОВОЇ ІНФРАСТРУКТУРИ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Анотація. Розглянуто застосування архітектури нульової довіри до цифрової інфраструктури закладу вищої освіти, де одночасно використовуються локальні інформаційні системи, хмарні сервіси, персональні пристрої та віддалений доступ. Обґрунтовано відмову від моделі, у якій сам факт перебування користувача у внутрішній мережі вважається достатньою підставою для довіри. Запропоновано поетапну модель впровадження: інвентаризація ресурсів, посилення ідентифікації, контроль стану пристроїв, мінімально необхідні права, сегментація доступу, централізоване журналювання та автоматизоване реагування. Показано, що нульова довіра є не окремим продуктом, а принципом побудови політик доступу, який потребує постійної перевірки користувача, пристрою, контексту та критичності ресурсу.

Ключові слова: нульова довіра, кібербезпека, ідентифікація, контроль доступу, заклад вищої освіти, цифрова інфраструктура.

Цифрова інфраструктура сучасного закладу вищої освіти істотно відрізняється від класичної корпоративної мережі з чітким периметром. Викладачі та здобувачі використовують хмарні сховища, системи дистанційного навчання, електронну пошту, відеоконференції, наукові сервіси та власні мобільні пристрої. Частина ресурсів розміщується локально, частина — у зовнішніх дата-центрах, а доступ до них здійснюється як із кампусу, так і з домашніх мереж. За таких умов модель безпеки, в якій внутрішня IP-адреса або підключення до університетської мережі автоматично підвищує рівень довіри, стає недостатньою.

NIST визначає zero trust як підхід, за якого користувачам і пристроям не надається неявна довіра лише через їх фізичне або мережеве розташування, а автентифікація та авторизація виконуються перед установленням сесії доступу до ресурсу (Rose et al., 2020). Практичне значення цього принципу для закладу

освіти полягає в перенесенні центру захисту з мережевого периметра на конкретні ресурси: облікові записи, навчальні платформи, фінансові системи, наукові дані, кадрову інформацію та адміністративні сервіси.

Першим етапом впровадження повинна бути не закупівля нового програмного забезпечення, а інвентаризація. Організація має знати, які сервіси існують, хто ними користується, які дані вони обробляють і які залежності мають. Для кожного ресурсу доцільно визначити власника, рівень критичності та групи користувачів. Без такого реєстру неможливо реалізувати принцип мінімально необхідних прав, оскільки адміністратор не має формалізованого уявлення про те, які саме права є необхідними. Особливої уваги потребують старі інформаційні системи, у яких доступ часто організований спільними обліковими записами або широкими мережевими дозволами.

Другим етапом є посилення ідентифікації та автентифікації. Для адміністративних, фінансових, кадрових і наукових систем доцільно застосовувати багатофакторну автентифікацію, а також централізоване керування життєвим циклом облікових записів. Створення, зміна ролі та блокування користувача повинні бути пов'язані з кадровими й освітніми процесами, щоб звільнений працівник або випускник не зберігав доступ довше, ніж це обґрунтовано. Для сервісних облікових записів необхідні окремі політики ротації секретів і заборона їх використання як звичайних користувацьких профілів.

Таблиця 1. Пріоритети впровадження zero trust у закладі освіти

Напрямок	Першочергова дія	Очікуваний результат
Ідентичність	MFA для критичних систем, централізовані ролі	Менший ризик компрометації облікових записів
Пристрої	Перевірка стану керованих пристроїв	Контекстний доступ до чутливих ресурсів
Мережа й застосунки	Сегментація, доступ за конкретним ресурсом	Обмеження бічного переміщення
Дані й аналітика	Класифікація даних, централізовані журнали	Краща простежуваність і реагування

Джерело: складено автором на основі Rose et al. (2020) та CISA (2023).

Третій компонент — стан пристрою. Однаковий обліковий запис не повинен отримувати однаковий рівень доступу з керованого службового ноутбука та з невідомого пристрою без актуальних оновлень. У політиці доступу можуть враховуватися шифрування диска, версія операційної системи, наявність засобів захисту, статус реєстрації пристрою та географічно або поведінково нетипові ознаки сесії. Водночас у закладі освіти важливо не перетворити контроль на необґрунтоване блокування навчального процесу. Тому критичні обмеження доцільно застосовувати передусім до чутливих ресурсів, залишаючи публічні навчальні матеріали доступними з мінімальними бар'єрами.

CISA пропонує оцінювати зрілість zero trust через п'ять основних напрямів: identity, devices, networks, applications and workloads, data, а також через наскрізні можливості visibility and analytics, automation and orchestration та governance (CISA, 2023). Для університету це дає практичну дорожню карту: спочатку забезпечити стабільну ідентифікацію та журналювання, потім сегментувати доступ до прикладних систем, а вже після цього автоматизувати реакцію на підозрілі події. Важливо, що зрілість не означає повної відмови від мережевих засобів захисту. Міжмережеві екрани, VPN, сегментація та захист кінцевих точок залишаються важливими, але вони працюють як частина багаторівневої моделі, а не як єдина межа довіри.

Ефективність впровадження доцільно оцінювати через вимірювані показники: частку критичних систем із багатофакторною автентифікацією, кількість привілейованих облікових записів, час блокування доступу після зміни статусу користувача, частку керованих пристроїв, повноту журналювання та середній час реагування на інцидент. Такий підхід дозволяє уникнути формального «впровадження zero trust» у вигляді одного продукту або проєкту без зміни політик.

Отже, для закладу вищої освіти архітектура нульової довіри є насамперед способом організувати доступ у середовищі, де периметр постійно змінюється. Найбільший ефект дає поступове впровадження від інвентаризації ідентичностей та ресурсів до контекстного контролю, сегментації й автоматизації. Критерієм успіху має бути не кількість придбаних засобів захисту, а зменшення необґрунтованих прав і здатність установи швидко підтвердити, хто, з якого пристрою і на якій підставі отримав доступ до конкретного ресурсу.

REFERENCES / СПИСОК ДЖЕРЕЛ

1. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0. U.S. Department of Homeland Security.
2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>