

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XI Всеукраїнської науково-практичної конференції
«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:
ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

18 грудня 2025 року



Полтава 2025

УДК 004.056.5:004.7:658.114.012.2

І.І. Тараненко, магістрант,

Г.В. Головка, к.т.н., доцент

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ZERO TRUST ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО ПІДПРИЄМСТВА

Малі та середні підприємства дедалі частіше стають мішенню автоматизованих кібератак, оскільки зловмисники використовують масові інструменти сканування та вибору вразливих цілей. У таких умовах традиційні периметрові моделі захисту вже не забезпечують належного рівня безпеки, а тому МСП потребують простішого та ефективнішого підходу до кіберзахисту. Концепція Zero Trust, заснована на відсутності довіри за замовчуванням і постійній перевірці доступу, дозволяє значно знизити ризики навіть без великих інвестицій [1].

Наукові дослідження підкреслюють, що Zero Trust є еволюцією класичних моделей безпеки і пропонує більш стійку архітектуру в умовах сучасних загроз. Однак у більшості академічних праць підхід описується з позицій великих організацій, що мають достатні ресурси для масштабних впроваджень. Для МСП такі моделі часто надто складні, а тому потребують спрощеного трактування, орієнтованого на доступність і мінімальні вимоги до технічної підготовки [2].

Огляди сучасних досліджень підтверджують, що МСП недостатньо представлені у світовій науковій літературі щодо Zero Trust, але при цьому саме вони є найбільш уразливими до атак через слабкі механізми автентифікації, відсутність сегментації, несистемне управління ідентифікації та недостатній моніторинг. У роботах з аналізу впроваджень Zero Trust наголошується, що для МСП ключовою проблемою є не відсутність інтересу, а складність реалізації та відсутність практичних поетапних моделей [3].

Низка досліджень, орієнтованих спеціально на малий бізнес, показує, що Zero Trust може приносити суттєву користь навіть при мінімальному впровадженні. Багатофакторна автентифікація, базова сегментація мережі, централізація доступу та регулярний моніторинг уже самі по собі значно скорочують кількість успішних атак. Проблеми впровадження здебільшого пов'язані з обмеженими бюджетами та відсутністю кваліфікованих спеціалістів, однак адаптовані покрокові моделі дозволяють частково компенсувати ці обмеження [4].

Аналітичні матеріали та рекомендації галузевих організацій демонструють, що для МСП найефективнішим є поетапний підхід: спочатку визначення активів, потім управління ідентифікації, далі посилення захисту пристроїв, автоматизація та безперервний моніторинг. Така модель

впровадження підтвердила свою ефективність у дослідницьких випробуваннях та реальних компаніях, де вона допомогла зменшити кількість інцидентів, підвищити дисципліну доступу та покращити загальну цифрову стійкість без значних фінансових витрат [5].

Zero Trust у контексті МСП — це передусім стратегія мислення, а не суто набір технологій. Вона дозволяє малим компаніям підвищувати цифрову стійкість та ефективність захисту, використовуючи інструменти, які вже є у їхньому розпорядженні. Поетапний підхід робить Zero Trust доступним навіть для бізнесів із мінімальним бюджетом, що робить його одним із найперспективніших методів побудови сучасного кіберзахисту.

ЛІТЕРАТУРА:

1. Microsoft. *Zero Trust Guidance for Small Businesses*. 2025. URL: <https://learn.microsoft.com/en-us/security/zero-trust/guidance-smb-partner/>
2. Korobeinikova T. *THE ZERO TRUST MODEL: Theory, Practice, and Prospect*. 2025. URL: <https://desymp.promonograph.org/index.php/sge/article/view/sge37-01-006/>
3. Mushtaq S., Mohsin M., Mushtaq M. *A Systematic Literature Review on Zero Trust*. 2025. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12526847/>
4. Abdelmagid A., Diaz R. *Zero Trust Architecture as a Risk Countermeasure for SMEs*. 2025. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12411126/>
5. Cloud Security Alliance. *Zero Trust Guidance for Small and Medium Size Businesses*. 2025. URL: <https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-small-and-medium-size-businesses-smbs/>

ZERO TRUST FOR SMALL AND MEDIUM ENTERPRISES

I. Taranenko, undergraduate,

G. Golovko, Ph.D., Associate professor

National University “Yuri Kondratyuk Poltava Polytechnic”