УДК 004.056:621.391

ОСНОВНІ НАПРЯМКИ УДОСКОНАЛЕННЯ ВПРОВАДЖЕННЯ ПОЛІТИКИ НУЛЬОВОЇ ДОВІРИ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Горяєв Р.О., Золотарьов В.А.
e-mail: rostyslav.horiaiev@nure.ua, vadym.zolotarov@nure.ua
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

The future of zero trust network architecture lies in advancing its adaptability, scalability, and integration with emerging technologies. Developing universal standards is essential to ensure consistent implementation and interoperability across diverse environments. AI and machine learning will play a pivotal role in automating threat detection, behavioral analysis, and dynamic policy enforcement, reducing reliance on manual processes. As quantum computing threatens traditional encryption, adopting quantum-resistant cryptography will enhance the resilience of ZTNA. Efforts to secure IoT and edge computing environments will involve lightweight authentication mechanisms and localized analytics for real-time threat mitigation.

Мета дослідження: з’ясувати основні напрямки удосконалення впровадження політики нульової довіри, проаналізувати всі напрямки за єдиним алгоритмом: мета, підхід, результати.

Політика нульової довіри передбачає постійну перевірку ідентифікації, аутентифікації та авторизації користувачів і даних в мережі. «Архітектура нульової довіри» постійно вдосконалюється та потребує інтеграції зі штучним інтелектом, впровадження квантової криптографії, покращення безпеки IoT, автоматизованого керування політиками та обміну інформацією про кіберзагрози. [1]. В результаті дослідження було виявлено 8 напрямів.

1. Використання штучного інтелекту (ШІ) та машинного навчання з метою виявлення кіберзагроз і кіберінцидентів, здійснення поведінкового аналізу та автоматизованого управління політиками. Моделі машинного навчання застосовуються для виявлення аномалій поведінки користувачів і систем, динамічної адаптації політик. Штучний інтелект використовується для оптимізації розподілу ресурсів систем автентифікації та моніторингу. Це покращить виявлення кіберзагроз, зменшить ручну роботу та покращить динамічну адаптація до змінних умов.

2. Застосування квантової криптографії для захисту інфокомунікацій та даних забезпечить підвищену стійкість до кібератак, полегшить виявлення втручання; унеможливіть несанкціоноване копіювання та підробку. Втім потребує подолання технічних викликів, таких як покращення дальності передачі та здешевлення обладнання.

3. Застосування архітектури нульової довіри на безпекове середовище інтернету речей та периферійних обчислень потребує розробки новітніх механізмів автентифікації та моніторингу для ресурсно обмежених пристроїв IoT, та використання периферійної аналітики для локалізованого виявлення загроз і впровадження політик. Це суттєво покращить безпеку для розподілених і ресурсно обмежених середовищ.

4. Використання технологій з підвищеною безпекою даних в галузі охорони здоров'я та платіжних системах. Передбачається використання таких технологій, як гомоморфне шифрування та диференціальна приватність, а також обмеження збирання даних мінімально необхідних для безпеки. Результат: підвищена довіра та дотримання норм конфіденційності.

5. Автоматизоване управління політиками безпеки спростить їхнє створення, управління та оновлення політик. Потрібна розробка інструментів для автоматизованої генерації політик на основі ролей користувачів, поведінки та умов середовища, а також використання підходу «policy as code» для забезпечення послідовності та масштабованості. Це забезпечить зменшення помилок і адміністративних витрат при управлінні політиками безпеки.

6. Контекстно-орієнтоване керування доступом передбачає обов'язкове використання геолокації, визначення стану пристрою, часу доступу та шаблонів активності користувача для визначення рівнів доступу, а також постійне оцінювання та адаптація дозволів у реальному часі. Що забезпечить більш точний і адаптивний контроль доступу користувачів і ресурсів.

7. Використання екосистем співпраці має забезпечити безперебійне впровадження архітектури нульової довіри шляхом розробки галузевих і міжвідомчих систем ідентичності для безпечної співпраці між організаціями, стандартизація API і протоколів для забезпечення сумісності забезпечить більш оптимізовані та безпечні міжорганізаційні взаємодії.

8. Покращення обміну інформацією про новітні кібератаки, кіберінциденти та кіберзагрози передбачає створення спеціальних платформ для безпечного та анонімного обміну даними, а також використання ШІ для агрегування та аналізу спільної інформації.

Висновки. Жодний з проаналізованих підходів самотужки не забезпечить ефективне впровадження політики нульового дня. Потрібно їхнє комплексне використання .

Список використаних джерел:

1. Denzel K. A survey of security in zero trust network architectures // GSC Advanced Research and Reviews. 2025. Vol. 22, No. 2. P. 182–214. URL: https://doi.org/10.30574/gscarr.2025.22.2.0036 (дата звернення: 02.03.2026).