УДК 004.056:004.738.5:004.8

Плахтій М.О. к.е.н., доцент, професор
ТОВ Приватний вищий навчальний заклад «УНІВЕРСИТЕТ СУЧАСНИХ ТЕХНОЛОГІЙ»

НЕЛІНІЙНА ПОСТКВАНТОВА АВТЕНТИФІКАЦІЯ В ФЕДЕРАТИВНИХ СИСТЕМАХ

Сучасний розвиток інформаційних технологій супроводжується трансформацією криптографічних стандартів і моделей управління ідентичностями. Стандартизація постквантових алгоритмів формує основу переходу до рішень, стійких до квантових атак [1]. Водночас їх впровадження у федеративні системи потребує врахування складної взаємодії криптографічних, поведінкових і контекстних компонентів безпеки.

У таких умовах автентифікаційні процеси доцільно розглядати як динамічні системи з нелінійними властивостями. Рівень довіри формується під впливом кількох груп факторів – криптографічних, поведінкових, контекстних і міждоменних. Зміна кожного з них впливає на загальний ризик непропорційно. Наведене підтверджує нелінійний характер функції прийняття рішень. Отже, модель автентифікації повинна забезпечувати адаптивну перебудову параметрів доступу.

Постквантові алгоритми обміну ключами та цифрового підпису утворюють квантово-стійке ядро системи [2]. Однак їх застосування не зводиться до заміни класичних примітивів. Необхідна інтеграція у комплексну архітектуру разом із механізмами ризик-орієнтованого контролю та адаптивного управління політиками [3]. У такій структурі криптографічні алгоритми забезпечують стійкість до квантових загроз. Натомість нелінійні механізми керування довірою забезпечують гнучкість і адаптивність.

Сучасні федеративні протоколи підтримують міждоменну взаємодію. Вона характеризується різними рівнями довіри та локальними політиками безпеки. Під час обміну атрибутами виникають нелінійні залежності між локальними та глобальними вимогами. Тому потрібна узгоджена модель, здатна поєднати класичні та постквантові механізми без втрати цілісності процесу. У цьому контексті нелінійна адаптація стає базовим принципом архітектури [4].

Автентифікацію запропоновано моделювати як нелінійну керовану систему зі зворотним зв'язком, у якій рівень довіри визначається на основі багатовимірного аналізу параметрів сесії. Адаптивне оцінювання ризику реалізується із застосуванням методів машинного навчання з урахуванням поведінкових і контекстних факторів, що забезпечує динамічну перебудову параметрів доступу. Інтеграція постквантових криптографічних алгоритмів формує квантово-стійке ядро

федеративної архітектури та забезпечує стійкість до квантових загроз. Запропонована модель поєднує криптографічний захист, адаптивне управління політиками та міждоменну координацію в єдину нелінійну структуру.

Наукова новизна полягає у формалізації постквантової автентифікації як цілісної нелінійної системи управління довірою, що забезпечує адаптивність і стійкість у федеративних середовищах. Запропонований підхід розглядає автентифікаційні процеси як єдину інтегровану архітектуру, у якій криптографічні та поведінкові механізми функціонують у межах нелінійної моделі. Така структура забезпечує узгоджене управління рівнем довіри та динамічну адаптацію параметрів доступу в умовах змінного середовища.

Таким чином, розроблення нелінійної моделі постквантової автентифікації у федеративних системах є актуальним науковим завданням. Реалізація такого підходу створює основу для побудови квантово-стійких, адаптивних і міждоменних механізмів керування довірою в умовах складної динаміки сучасних інформаційних середовищ.

Список використаних джерел

1. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://csrc.nist.gov/projects/post-quantum-cryptography.

2. National Institute of Standards and Technology. (2024, August 13). NIST releases first 3 finalized post-quantum encryption standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

3. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 24760-1:2025 Information security, cybersecurity and privacy protection – A framework for identity management. Part 1: Core concepts and terminology (3rd ed.). https://www.iso.org/standard/24760-1.

4. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв’язку*. 2025. № 4 (82). С. 138–143. DOI: https://doi.org/10.26906/SUNZ.2025.4.138. URL: https://journals.nupp.edu.ua/sunz/article/view/4119 (дата звернення: 04.02.2026).