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 004.021:004.89:004.056.5
Ю.В. Калашнікова, *асистент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

МОДЕЛЬ АДАПТИВНОГО КРИПТОГРАФІЧНОГО УПРАВЛІННЯ ДОСТУПОМ У МУЛЬТИДОМЕННИХ СИСТЕМАХ

Сучасний розвиток IT супроводжується стрімким зростанням ролі цифрових систем у критично важливих галузях, зокрема у промисловості, енергетиці, транспорті та сфері державного управління. Впровадження концепцій Internet of Things, cyber-physical systems і хмарних обчислень зумовило формування мультидоменних кіберінфраструктур, у межах яких одночасно функціонують гетерогенні пристрої, сервіси та користувачі з різними рівнями доступу і довіри. У таких умовах особливе значення набуває управління спец користувачами, наділеними розширеними привілеями, оскільки їх компрометація може призвести до системних порушень безпеки та втрати керованості критичними процесами.

Аналіз існуючих підходів до керування доступом свідчить, що більшість з них базується на статичних політиках авторизації та заздалегідь визначених ролях. Подібні моделі не враховують динамічні зміни контексту використання ресурсів, поведінкові особливості користувачів і не забезпечують оперативного реагування на аномальні дії. Як наслідок, системи залишаються вразливими до внутрішніх атак, несанкціонованої ескалації привілеїв та зловживання сервісними обліковими записами, що особливо критично для розподілених IoT- і SCADA-середовищ.

Додатковим ускладнюючим фактором є необхідність криптографічного захисту інформаційних потоків у гібридних мережах з різнорідними обчислювальними ресурсами та каналами зв’язку. Інтеграція алгоритмів симетричного шифрування, зокрема AES, у такі середовища потребує забезпечення балансу між криптографічною стійкістю, обчислювальною ефективністю та мінімальними затримками автентифікації. При цьому ключовими завданнями залишаються уніфіковане керування ключовим матеріалом, контроль життєвого циклу сеансів доступу та забезпечення міждоменного довірчого обміну.

У цьому контексті перспективним напрямом є застосування інтелектуальних механізмів адаптації доступу, заснованих на методах ML. Поведінковий аналіз активності спеціальних користувачів дозволяє формувати динамічні профілі доступу на основі часових, просторових і функціональних ознак, виявляти відхилення від нормальної поведінки та автоматично коригувати рівень привілеїв. Поєднання таких підходів із криптографічними протоколами створює основу для побудови

самоадаптивної архітектури управління доступом, здатної забезпечити високий рівень безпеки без втрати продуктивності.

У роботі запропоновано архітектурно-криптографічну модель управління системами спец користувачів з інтелектуальною адаптацією доступу. Модель орієнтована на застосування в мультидоменних кіберінфраструктурах і поєднує механізми симетричного шифрування DES/AES із модулями поведінкової аналітики та динамічного керування політиками доступу. Наведена архітектура передбачає можливість інтеграції в гетерогенні середовища, включно з IoT-платформами, SCADA-системами та урядовими дата-центрами, з урахуванням обмежень пропускної здатності та обчислювальних ресурсів.

Експериментальні дослідження підтвердили доцільність застосування алгоритмів AES-256 у режимах автентифікованого шифрування з використанням апаратного прискорення, зокрема технологій AES-NI та HSM. Отримані результати засвідчили, що запропонована модель забезпечує високий рівень криптографічної стійкості при збереженні низьких затримок автентифікації та лінійної масштабованості продуктивності. Навантажувальні тести показали стабільну роботу системи за умов одночасного обслуговування тисяч привілейованих сесій без деградації показників SLA.

Окрему увагу приділено сценаріям динамічної ротації ключів і федеративної автентифікації у розподілених середовищах. Результати експериментів засвідчили здатність моделі підтримувати безперервність криптографічних процесів і забезпечувати час реакції системи менше однієї секунди навіть у складних SCADA/IoT-конфігураціях. Це підтверджує практичну придатність запропонованого підходу для використання у критично важливих інформаційних системах державного та промислового призначення.

Узагальнюючи отримані результати, можна стверджувати, що запропонована архітектурно-криптографічна модель створює науково обґрунтовану основу для побудови адаптивних систем управління привілеями спеціальних користувачів. Поєднання криптографічних механізмів із інтелектуальною адаптацією доступу підвищує кіберстійкість мультидоменних інфраструктур і знижує ризики внутрішніх загроз. Подальші дослідження доцільно спрямувати на розвиток адаптивної криптографії, енергетично ефективних рішень для ресурсно обмежених пристроїв, інтеграцію квантово-стійких алгоритмів та створення прогнозних модулів моніторингу на базі AI.

ЛІТЕРАТУРА:

1. NIST. Post-Quantum Cryptography (Projects). National Institute of Standards and Technology (NIST). Available at: https://csrc.nist.gov/projects/post-quantum-cryptography

2. Zhyvylo, Ye. Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences / Yevhen Zhyvylo, Vladyslav Kuz // Theoretical and Applied Cybersecurity : scientific journal. – 2023. – Vol. 5, Iss. 2. – Pp. 68–80. – https://doi.org/10.20535/tacs.2664-29132023.2.280377

MODEL OF ADAPTIVE CRYPTOGRAPHIC ACCESS CONTROL IN MULTIDOMAIN SYSTEMS

Y. Kalashnicova, Assistant
National University "Yuri Kondratyuk Poltava Polytechnic"