doi: https://doi.org/10.15407/visn2023.08.065

ЦИФРОВА АВТЕНТИФІКАЦІЯ: ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ

Стенограма доповіді на засіданні Президії НАН України 31 травня 2023 року

АНІСІМОВ Анатолій Васильович — член-кореспондент НАН України, головний науковий співробітник Міжнародного науково-навчального центру інформаційних технологій та систем НАН України і МОН України, декан факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка

У доповіді акцентовано увагу на актуальності розроблення методів, алгоритмів та протоколів цифрової автентифікації, що стає особливо важливим сьогодні, в умовах повномасштабної російської воєнної агресії проти України. Зазначено, що одним із пріоритетних напрямів наукової діяльності Міжнародного науково-навчального центру інформаційних технологій та систем НАН України і МОН України є захист інформації, зокрема розвиток теорії і практики цифрової автентифікації. Створено нові методи цифрової автентифікації, які ґрунтуються на сучасних досягненнях криптографії з відкритими ключами і враховують виклики й загрози, які нині виникають у глобальному кіберпросторі.

Шановний Анатолію Глібовичу!
Шановне зібрання!
Дозвольте представити до вашої уваги доповідь, присвячену обговоренню досягнень та перспектив розвитку цифрової автентифікації.

Обсяг використання інформаційно-комунікаційних технологій у діяльності сучасного суспільства постійно зростає, глобалізується світовий інформаційний простір. За даними дослідження, проведеного корпорацією Google, у 2023 р. зафіксовано 5,18 млрд користувачів Інтернету, що відповідає 64,6 % людства. З кожним роком число користувачів зростає. Крім того, експоненційно збільшується кількість соціальних, корпоративних, спеціальних мереж та засобів інформаційно-комунікаційних технологій. Останнім часом посилюється також залежність людства від широкого впровадження технологій штучного інтелекту. Виникла навіть нова технологічна галузь, яку називають «Інтернет речей» (Internet of Things — IoT).

У зв'язку з формуванням та розвитком глобального кіберпростору, цифровою трансформацією та побудовою цифрового майбутнього світу протягом останніх десятиліть у цифровому середовищі виникли нові загрози та ризики. Тому безпека національного кіберпростору, захист національних інформа-

ційних ресурсів та критичної інфраструктури стали пріоритетними завданнями для кожної країни.

За даними Symantec — американської компанії з виробництва програмного забезпечення в галузі інформаційної безпеки, у 2022 р. було виявлено понад 5,8 млрд спроб шахрайства, пов'язаного з ідентифікацією, зокрема йдеться про фішингові атаки, шахрайські вебсайти, компрометацію облікових записів тощо. Ці статистичні дані демонструють поширеність і масштаб проблеми та важливість розроблення методів захисту від кібератак, шахрайства, несанкціонованого доступу. Цифрова автентифікація є одним із засобів боротьби з такими загрозами та гарантування безпеки в онлайн-середовищі.

Актуальність розроблення методів, алгоритмів та протоколів цифрової автентифікації полягає в їх важливості для безпеки в глобальному кіберпросторі, захисту конфіденційної інформації та персональних даних, поліпшення користувацького досвіду та виконання регуляторних вимог. Отже, автентифікація є ефективним інструментом у боротьбі з кіберзагрозами та дотриманні безпеки в цифровому просторі, а також стає надзвичайно актуальним напрямом у сучасному світі, де все більше й більше послуг, транзакцій та комунікацій зосереджено в онлайн-середовищі.

Однак перш ніж почати розмову про автентифікацію, варто коротко зупинитися на термінології. Слід розрізняти два основні поняття в інформаційній безпеці — терміни «ідентифікація» і «автентифікація». Ідентифікація — це процедура розпізнавання системою суб'єкта (користувача, програми, процесу) з використанням певного ідентифікатора (наприклад, логіна), за допомогою якого суб'єкт декларує про себе. Автентифікація — це процедура цифрового доведення того, що суб'єкт є саме тим, за кого він себе видає, тобто встановлення відповідності суб'єкта пред'явленому ним ідентифікатору, що досягається за допомогою автентифікатора (наприклад, складного пароля, ключа, біометричних даних тощо). Обидві ці процедури потрібні для авторизації — надання визначеному суб'єкту певного рівня доступу до системи і певних повноважень, тобто прав на виконання тих чи інших дій (статус адміністратора ресурсу, користувача тощо).

Найпростішим способом автентифікації є використання пароля. Цей метод був поширений на початку розвитку інформаційно-комунікаційних технологій, проте на сьогодні він є ненадійним. Втім, існують деякі засоби підвищення захищеності зберігання і передавання паролів, зокрема використання випадкових параметрів, або хеш-функцій, які маскують самі паролі, або системи віддаленої ідентифікації через довірчий сервер. При цьому автентифікація може бути однобічною, двобічною або трибічною, як у випадку застосування довірчого сервера. Іншим способом автентифікації є використання різних сертифікатів, цифрових ключів, електронного цифрового підпису. Є також біометричний спосіб, в основі якого лежить аналіз унікальних характеристик людини, наприклад відбитків пальців, малюнку райдужки або сітківки ока, голосу, характерних рис обличчя тощо.

У 1990-х роках виник досить цікавий спосіб автентифікації, оснований на протоколах з нульовим розголошенням. Його суть полягає в доведенні однією стороною іншій стороні, що вона знає якесь твердження, без розкриття будь-якої іншої інформації, крім достовірності цього твердження. Цей на перший погляд парадоксальний метод став доступним для практичного використання завдяки відкриттю криптографії з публічними (відкритими) ключами.

І нарешті напрям, який зараз активно розвивається в Міжнародному науково-навчальному центрі інформаційних технологій та систем НАН України та МОН України, — це криптографія типу «свій-чужий», що також належить до криптографії з публічними ключами. В ній застосовують різні алгоритми, які ґрунтуються на різноманітних методах захисту інформації, зокрема на асиметричних криптографічних методах та використанні хеш-функцій. При цьому відправник використовує публічний ключ для шифрування інформації, а одержу-

вач для розшифрування застосовує приватний ключ. Кожна пара таких асиметричних ключів унікальна, що гарантує, що повідомлення може прочитати лише той, хто має відповідний приватний ключ. Тому публічний ключ можна використовувати для шифрування даних при передачі відкритими каналами зв'язку без загрози для безпеки інформації, тобто асиметричні алгоритми забезпечують вищий рівень захисту, ніж симетричні.

Криптографію з публічними ключами сьогодні широко використовують для захисту передачі інформації незахищеними каналами зв'язку, автентифікації за допомогою електронного цифрового підпису, проведення транзакцій з криптовалютами, у блокчейн-технологіях, а також для автентифікації в мережах «Інтернету речей».

В умовах повномасштабної російської агресії проти України особливого значення набуває вирішення завдань із захисту інформації. За даними корпорації Microsoft, крім атак на українські сайти, які почалися з 24 лютого 2022 р., російські хакери здійснили в цей період 128 нападів на ресурси 42 країн. У 29 % випадків ці кібератаки досягали своєї мети.

Україна стала мішенню активних кібератак з боку хакерських груп, спрямованих на знищення інфраструктури та поширення дезінформації. Цифрова автентифікація є ефективним засобом захисту від таких атак, оскільки вона дає змогу перевірити та підтвердити ідентичність користувачів й унеможливити несанкціонований доступ до систем, ресурсів та інфраструктури.

Актуальним є також питання боротьби зі спробами отримати несанкціонований доступ до конфіденційної інформації. Цифрова автентифікація відіграє важливу роль у захисті такої інформації, зокрема державних та комерційних таємниць, забезпечуючи ідентифікацію користувачів і перевірку їхньої автентичності перед наданням доступу до конфіденційної інформації.

Цифрова автентифікація є однією з надважливих складових сучасної кібербезпеки, що дає можливість керувати процесами прийняття рішень і авторизації доступу до критично важливих ресурсів. Слід зазначити, що сучасний рівень технології цифрової автентифікації потребує наявності фахівців з глибокими знаннями з математики, теорії інформації, сучасної криптографії, квантових обчислень і штучного інтелекту.

Міжнародний науково-навчальний центр інформаційних технологій та систем НАН України та МОН України має багаторічний досвід виконання науково-технічних робіт у галузі інформаційно-комунікаційних технологій, кібернетичної безпеки, інтелектуального кодування інформації з метою її оптимального відображення під час передачі та аналізу цілісності, комп'ютерного розуміння природної мови. Центр також бере участь у розбудові системи національного спротиву в інформаційному, психологічному та кібернетичному просторі і підготовці кваліфікованих фахівців з кібербезпеки.

Як я вже говорив, у Центрі розроблено методи цифрової автентифікації, що ґрунтуються на сучасних досягненнях криптографії з відкритими ключами та враховують нинішні виклики й загрози, які виникають у глобальному кіберпросторі. Нові підходи до захисту інформації та ідентифікації підвищують ефективність і надійність систем автентифікації. Запропоновані методи мають істотну перевагу над уже відомими методами, яка полягає насамперед у простоті реалізації. Алгоритми побудовані так, що їх можна реалізувати на різних сучасних мовах програмування. Вибір мови програмування виноситься на етап конкретного впровадження після узгодження алгоритмів, а використання швидких хеш-функцій, що мають швидкий алгоритм обчислення, значно скорочує час оброблення автентифікаційних запитів. Ці алгоритми допускають апаратну реалізацію, що уможливлює їх використання на різних пристроях. Це сприяє швидкому й ефективному впровадженню систем автентифікації. Розроблені алгоритми мають високий ступінь захисту від зловмисних атак, оскільки вони засновані на математичних принципах, що враховують важливі аспекти безпеки.

Розроблені алгоритми та протоколи автентифікації на основі криптографічних хеш-функцій забезпечують швидку й безпечну ідентифікацію об'єктів і засобів у різних сферах застосування, таких як комп'ютерні системи та мережі зв'язку. Отримані нами результати апробовано і впроваджено в підрозділах Сил територіальної оборони Збройних Сил України.

Майбутня робота у сфері цифрової автентифікації на базі криптографії з відкритими ключами передбачає також розвиток напряму квантової криптографії. З появою квантових обчислень особливо важливим стає розроблення алгоритмів та протоколів для дотримання вимог безпеки цифрової автентифікації. Квантова криптографія може використовувати принципи квантової механіки для створення криптографічних протоколів, стійких до зламу навіть при застосуванні квантових комп'ютерів. Зокрема, квантові ключі можна використовувати для забезпечення конфіденційності та цілісності даних.

Важливим є продовження досліджень для потреб оборони держави, де безпека, конфіденційність та ідентифікація відіграють ключову роль у захисті інформації й забезпеченні операційної ефективності. Завдяки новим методам, алгоритмам та протоколам можна підвищити ефективність та швидкість цифрової автентифікації на базі криптографії з відкритими ключами. Більш швидкі алгоритми підпису і шифрування, оптимізовані протоколи передачі даних дадуть змогу забезпечити швидку й ефективну автентифікацію без затримок. З цією метою передбачено розширити співпрацю Центру з українськими спецслужбами та Міністерством цифрової трансформації України.

Дякую за увагу!

За матеріалами засідання
підготувала О.О. Мележик

Anatoly V. Anisimov

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

International Research and Training Center for Information Technologies and Systems of the National Academy of Sciences of Ukraine and Ministry of Education and Science of Ukraine, Kyiv, Ukraine

ORCID: https://orcid.org/0000-0002-1467-2006

DIGITAL AUTHENTICATION: ACHIEVEMENTS AND PROSPECTS

Transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, May 31, 2023

The report focuses on the relevance of the development of digital authentication methods, algorithms and protocols, which is becoming especially important today, in the conditions of full-scale Russian military aggression against Ukraine. It is noted that one of the priority scientific activity areas of the International Research and Training Center for Information Technologies and Systems of the National Academy of Sciences of Ukraine and the Ministry of Education and Science of Ukraine is information protection, in particular, the development of the theory and practice of digital authentication. New digital authentication methods have been created, which are based on modern advances in public-key cryptography and take into account the challenges and threats that currently arise in global cyberspace.

Cite this article: Anisimov A.V. Digital authentication: achievements and prospects. *Visn. Nac. Akad. Nauk Ukr.* 2023. (8): 65—68. https://doi.org/10.15407/visn2023.08.065