РАКОЇД Дмитро Володимирович
ЄРЬОМІН Іван Юрієвич
ЯРОЩУК Дмитро Миколайович
Київський інститут Національної гвардії України

ЕВОЛЮЦІЯ СПОСОБІВ І МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Інформація завжди була і є до тепер одним із найцінніших ресурсів: від особистих даних і комерційних таємниць до безпеки окремої держави. Захист інформації пройшов довгий шлях еволюції – від найпримітивніших прийомів приховування повідомлень до складних математичних алгоритмів і квантових технологій.

З античних часів застосовувалися спроби приховати зміст повідомлення. Так, у V ст. до н. е. в Спарті використовували «скіфалу» – дерев'яний циліндр, на який намотували папірус із зашифрованим текстом. У І ст. до н. е. Гай Юлій Цезар використовував простий замінний шифр із зсувом трьох букв, відомий нині як «шифр Цезаря». Вже в 1467 році в Італії Леон Баттіста Альберті винайшов поліалфавітний шифрний диск, що давав змогу змінювати зсув у ході шифрування, а в 1586 році Жан Віженер описав шифр, який у XIX ст. отримав його ім'я. Ці методи дозволяли захищати паперові документи та послання на обмеженій території й в умовах низької складності криптоаналізу.

Наприкінці XVIII – на початку XIX ст. з розвитком телеграфії постало питання безпечної передачі даних на великі відстані. У 1844 році Семюел Морзе продемонстрував перший комерційний телеграфний зв'язок між Вашингтоном і Балтимором, але для захисту повідомлень використовувалися оперативні заходи (окремі лінії, кодові таблиці), аніж складні криптографічні схеми. У 1917 році розкриття британською розвідкою «Циммерманівського телеграму» (Zimmermann Telegram) стало одним із перших прикладів успішного криптоаналізу великих обсягів телеграфних даних.

Найбільш відомим механічним пристроєм захисту інформації стала німецька «Еніґма», розроблена в 1923 році інженером Артуром Шербіусом. Прилад складався з трьох-п’яти роторів, що змінювали електричні з’єднання й забезпечували надзвичайно велику кількість можливих ключів. Лише завдяки спільним зусиллям криптоаналітиків із Польщі, Великої Британії та США вдалося зламати «Еніґму» наприкінці 1930-х – початку 1940-х років, що значно вплинуло на перебіг Другої світової війни.

З другої половини XX століття з поширенням електронних обчислювальних машин почалася нова ера криптографії. У 1975 році Національний інститут стандартів і технологій США (NIST) опублікував перший федеральний стандарт шифрування – DES (Data Encryption Standard), затверджений як FIPS-46 у 1977 році. DES використовував 56-бітний симетричний ключ і працював із блоками по 64 біти. Уже наприкінці 1970-х з’ясувалося, що 56 біт недостатньо для протидії брутфорсу: 1998 року проект Electronic Frontier Foundation зібрав спеціальну машину, яка змогла зламати DES за 56 годин.

У 1976 році в журналі «IEEE Transactions on Information Theory» були опубліковані статті Уітфілда Діффі та Мартіна Геллмана, де вони запропонували ідею обміну ключами через незахищений канал, заклавши основу асиметричної криптографії. Незабаром Рон Рівест, Аді Шамір і Леонард Адлеман реалізували практичний алгоритм RSA (1977 рік), що ґрунтувався на складності факторизації великих чисел. RSA працює з ключами довжиною від 1024 до 4096 біт, що забезпечує значно вищий рівень захисту порівняно з DES.

У 1992 – 1995 роках були розроблені геш-функції MD5 і SHA-1, які протягом кількох років використовувалися для забезпечення цілісності даних. Однак у середині 2000-х були виявлені колізії в MD5 (2004 рік) і SHA-1 (2005 рік), що призвело до поступового їхнього виведення з експлуатації.

У 2001 році NIST оголосив конкурс на новий стандарт шифрування, і в результаті у жовтні 2001 року був затверджений алгоритм AES (Advanced Encryption Standard). Переможцем стала версія Rijndael бельгійських

криптографів Вінсента Рейменса та Йоана Дменса. AES підтримує ключі довжиною 128, 192 і 256 біт та блоки по 128 біт, що дозволяє забезпечувати як високу продуктивність, так і стійкість проти криптоаналізу.

Зі стрімким розвитком мережі Інтернет виникла потреба у стандартах захисту передаваних даних. У 1994 році Netscape представила SSL (Secure Sockets Layer) версії 2.0, а в 1996 році – SSL 3.0. У 1999 році IETF опублікувала TLS 1.0 (Transport Layer Security), який став наступником SSL. На сьогодні найпоширеніші версії - TLS 1.2 (2008) і TLS 1.3 (2018), що забезпечують швидке встановлення з'єднання, використання еліптичних кривих для обміну ключами та захист від атак відтворення (replay).

Цифрова стеганографія дозволяє приховувати інформацію в медіафайлах (зображеннях, аудіо, відео). Один із відомих методів – LSB (Least Significant Bit), що змінює найменш значущі біти пікселів, забезпечуючи пропускну здатність близько 0,1 – 0,5 КБ на 1 КБ зображення без помітних артефактів.

Технологія блокчейн, започаткована у 2008 році у статті Сатоші Накамото, дала змогу створювати розподілені реєстри з криптографічним захистом кожного блоку через хеш-функції та цифрові підписи. Станом на 2025 рік мережа Bitcoin містить понад 800 000 блоків, а Ethereum - понад 15 млн, що підтверджує стійкість і надійність цих систем.

У 1984 році Чарльз Беннетт і Жиль Брассар вперше описали протокол BB84 для квантової передачі ключів. Комерційні системи квантової криптографії з'явилися в 2004 році (ID Quantique), а в 2016 році Китай запустив у космос перший квантовий супутник Micius, що забезпечує захищену передачу ключів на відстань понад 1200 км.

Одночасно з розвитком квантової криптографії активізувалася робота над пост-квантовими алгоритмами, стійкими до атак на квантових комп'ютерах. У 2016 році NIST оголосив конкурс на стандартизацію пост-квантових алгоритмів, у 2022-2024 роках завершив відбір п'яти алгоритмів (серед них CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+), які вже рекомендовані для впровадження в інформаційних системах.

У найближчі роки очікується подальше поширення гомоморфного шифрування (перше практичне рішення представив Крейг Джентрі 2009 року), що дозволяє обробляти зашифровані дані без розшифровки. Також активно досліджуються схеми секретного розподілу (secret sharing), мультипартійних обчислень (MPC) та забезпечення приватності даних у хмарних середовищах. Поширення Інтернету речей (IoT) вимагає розробки легких криптографічних алгоритмів для малопотужних пристроїв, а впровадження штучного інтелекту стимулює створення систем виявлення аномалій у реальному часі.

Еволюція способів і методів захисту інформації відображає розвиток людського суспільства: від механічних і паперових технологій до високотехнологічних криптографічних систем і квантових протоколів. Кожен історичний етап був зумовлений конкретними викликами – війнами, технологічними проривами, появою нових каналів зв'язку. Сучасна парадигма інформаційної безпеки – це поєднання симетричних і асиметричних алгоритмів, протоколів захисту мережевого рівня, біометрії та блокчейн-технологій, а в перспективі – квантових і пост-квантових рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Печенюк А. В. Інформаційна безпека України як складова національної безпеки. URL: https://www.ndifp.com/1561.

2. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. Інформація і право, 2018. № 1 (24). С. 127-132.

3. Архипов О. Є., Луценко В. М., Худяков В. О. Захист інформації в телекомунікаційних мережах та системах зв'язку: Учеб. пособие. – К.: Політехніка, 2003. – 38 с.