УДК 004.056.55
Постоленко М.О.[1], Романенко С.М.[2]
[1] студ. гр. БК-713м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

КРИПТОГРАФІЧНІ РІШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Криптографія була однією з перших дисциплін у рамках інформаційної безпеки. Починаючи з античних часів, військові, дипломати та шпигуни використовували різні пристрої та засоби шифрування, дешифрування та передачі секретної інформації. У середні віки криптографія продовжила розвиток і стала складнішою й різноманітнішою, включаючи різні форми транспозиційних та підстановочних шифрів. Із початку XX століття технології криптографії еволюціонували безперервним потоком механічних, електронних та математичних інновацій, досягнувши такого ступеню розвитку, що тепер вони вкоренилися в нашому повсякденному житті скрізь, ставши непомітною, але невід'ємною частиною практично будь-якої роботи із цифровою інформацією. Сучасні криптографічні рішення відіграють ключову роль у захисті даних та систем їхньої обробки. Криптографічні технології присутні в багатьох системах інформаційної безпеки. У цій роботі коротко описуються деякі криптографічні рішення із загальноприйнятими абревіатурами, а для неусталених абревіатур використовуються повні назви.

Криптографічні рішення

Можна виділити кілька класів загальних та спеціалізованих криптографічних рішень, серед яких такі:

ES (Encryption Solutions) – загальний клас рішень, що захищають дані, перетворюючи їх на зашифровану форму, доступ до якої можливий лише за

допомогою правильного ключа. Рішення щодо шифрування з'явилися в докомп'ютерну епоху. Вони охоплюють широкий спектр інструментів і технологій, призначених для шифрування даних, що перебувають у стані спокою, так і переданих. Це може включати в себе програми шифрування, протоколи шифрування для безпечного зв'язку (наприклад, SSL/TLS для інтернет-трафіку) і сервіси шифрування, що надаються хмарними провайдерами. Ціль цих рішень – забезпечити конфіденційність та цілісність даних шляхом перетворення читаних даних у нечитаний формат, який можна звернути тільки за допомогою правильних ключів розшифровки.

FDE (Full Disk Encryption) – це клас програмних чи апаратних рішень, призначених для шифрування всіх даних на жорсткому диску комп'ютера чи іншого пристрою. Такий підхід забезпечує захист інформації на рівні диска, включаючи системні файли, програми та дані. Основна мета FDE – забезпечення конфіденційності та захисту даних на пристрої від несанкціонованого доступу, особливо у разі втрати або крадіжки. Різновиди FDE – програмні та апаратні рішення. Системи FDE пов'язані з технологією TPM (див. далі). Одна з перших систем FDE Jetico BestCrypt була розроблена у 1993 році. Найпоширенішими рішеннями FDE, вбудованими в операційні системи, є Microsoft BitLocker та Apple FileVault.

Password Management Tools (Password Managers) – інструменти, призначені для спрощення та покращення процесів створення та зберігання паролів. Функції менеджерів паролів – генерація сильних паролів, зберігання та впорядкування паролів, автоматичне заповнення форм, зміна паролів. Різновиди інструментів управління паролями – персональні менеджери паролів; менеджери паролів для команд, що надають функціонал спільного використання паролів у робочих групах; менеджери привілейованих паролів; корпоративні менеджери паролів (EPM) Перший програмний менеджер паролів Password Safe був створений Брюсом Шнайєром в 1997 році як безкоштовна утиліта для Microsoft Windows 95. Станом на 2023 рік найчастіше використовуваним менеджером паролів був вбудований менеджер паролів Google Chrome.

EPM (Enterprise Password Management) – це розвиток менеджерів паролів у застосуванні на всю організацію. Ці рішення призначені для централізованого управління паролями, надаючи управління, моніторинг та захист привілейованих облікових записів як власних, так і сервісних облікових записів в організаціях. Функції EPM – централізоване керування паролями, автоматичне оновлення паролів, відстеження активності паролів, регулярний аудит для забезпечення відповідності політикам безпеки, керування доступом на основі ролей. Різновиди EPM – наземні та хмарні. Рішення для управління паролями в корпоративному середовищі почали розвиватися на початку 2000-х років.

TRSM (Tamper-Resistant Security Module) – це загальна назва пристроїв, призначених для особливої стійкості до фізичного втручання та несанкціонованого доступу. Ці модулі часто включають додаткові заходи фізичної безпеки, такі як: механізми самознищення, щоб запобігти фізичним атакам або несанкціонованому доступу до ключів шифрування та криптографічних операцій, які вони виконують. TRSM необхідні у середовищах, де безпека є основною турботою, таких як: військові чи фінансові установи. Найпростішими прикладами TRSM є платіжні смарт-картки, які з'явилися у 1970-х роках. Також прикладами TRSM є POS-термінали та пристрої HSM.

HSM (Hardware Security Module) – фізичний обчислювальний пристрій, який захищає секрети та керує ними. HSM з'явилися наприкінці 1970-х років. Апаратні модулі безпеки зазвичай забезпечують безпечне керування найважливішими криптографічними ключами та операціями. HSM використовуються для генерації, зберігання та керування ключами шифрування в безпечній формі, пропонуючи більш високий рівень безпеки, ніж програмне керування ключами, оскільки ключі зберігаються у захищеному від злому апаратному пристрої. HSM широко використовуються у середовищах з високим рівнем безпеки, таких як: фінансові установи, державні агенції та великі підприємства, де захист чутливих даних має вирішальне значення.

KMS (Key Management Systems) – це рішення, призначені для централізованого управління криптографічними ключами, які використовуються для шифрування даних. Основним їхнім завданням є забезпечення безпеки, доступності та управління життєвим циклом ключів. KMS автоматизують процеси створення, розподілу, зберігання, ротації та знищення ключів. Вони інтегруються з різними програмами та інфраструктурою, надаючи централізований контроль над шифруванням у підприємствах. Ідея централізованого управління криптографічними ключами почала розвиватися у 1970-х роках разом із зростанням використання криптографії, але конкретні системи KMS почали активно розроблятися та впроваджуватися у 1990-х та 2000-х роках.

PKI (Public Key Infrastructure) – це система, яка використовується для створення, керування, розподілу, використання та зберігання цифрових сертифікатів та відкритих криптографічних ключів. Вона забезпечує безпечне цифрове підписування документів, шифрування даних та автентифікацію користувачів або пристроїв в електронних системах. PKI є ключовим елементом у забезпеченні безпеки мережевих комунікацій та транзакцій, дозволяючи учасникам конфіденційно обмінюватися даними та підтверджувати справжність один одного. PKI надає набір інструментів для управління асиметричними ключами та сертифікатами як у рамках окремих

організацій, так і цілих держав. Цим рішення PKI відрізняються від рішень KMS, які зосереджені на гнучкішому управлінні ключами, проте зазвичай лише в рамках одного підприємства. Історія PKI розпочалася у 1970-х роках з розробки асиметричного шифрування. Концепція PKI у сучасному розумінні була розроблена та стандартизована у 1990-х роках. З появою блокчейну Ethereum у 2015 році почали розвиватись децентралізовані PKI.

SSE (Server-Side Encryption) – метод шифрування даних, що зберігаються на стороні сервера, що використовується з початку 2000-х років для підвищення безпеки даних. Шифрування на стороні сервера є шифрування даних на накопичувачах сервера. Ключі шифрування керуються самим сервером або центральною системою керування ключами. Це гарантує доступ до даних лише уповноважених осіб. SSE особливо ефективний для захисту конфіденційних даних у хмарному сховищі, оскільки запобігає несанкціонованому доступу навіть у разі компрометації фізичних пристроїв зберігання.

TPM (Trusted Platform Module) – це апаратний компонент, який забезпечує безпечне зберігання криптографічних ключів, що використовуються для шифрування та захисту інформації на комп'ютері або іншому пристрої. TPM встановлюється на материнську плату пристрою або вбудований процесор. Уперше концепція TPM була представлена консорціумом Trusted Computing Group (TCG) та стандартизована ISO у 2009 році. З того часу TPM став стандартним компонентом у багатьох комп'ютерах, особливо в корпоративному секторі, де вимоги до безпеки особливо високі.

ZKP (Zero-Knowledge Proof) – технологія доказу з нульовою довірою використовується для виконання завдання комунікацій, коли одній стороні потрібно переконати іншу сторону, що перша знає якусь таємницю, не розкриваючи цієї таємниці, крім достовірного факту її наявності. У розвиток технології ZKP у 1980-х роках зробили внесок Сільвіо Мікалі, Шафі Голдвассер, Одед Голдрейх, Аві Вігдерсон та Чарльз Ракофф. Починаючи з 2020 року, у рамках методу ZKP створено пост-квантові системи безпеки, тобто системи, стійкі до криптоаналізу на квантових комп'ютерах. Технологія ZKP знаходить все більше застосувань, від безпеки транзакцій та автентифікації до забезпечення конфіденційності в блокчейн-системах та інших додатках, де важливий захист особистих даних та конфіденційності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горбенко, І.Д., Горбенко, Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: підручник для вищих навч. закладів. – Харків: Форт, 2013. – 880 с.