**Тема 3. Захист інформації на рівні апаратного забезпечення**

План

1. Апаратні ключі

2. Системи сигналізації

3. Засоби блокування пристроїв та інтерфейсів вводу-виводу інформації

Інформаційні ресурси в сучасних умовах є одним із найважливіших інструментів діяльності людського суспільства. Саме тому проблема захисту інформації на сьогоднішній день є досить актуальною. Одним із підходів, щодо вирішення завдань захисту інформації є застосування апаратного забезпечення. Актуальність цієї проблеми не зменшується, а стає дедалі необхідною.

Так, до апаратних пристроїв, що запобігають викраденню паролів та надійно захищають навіть від фішингу та фізичного доступу до пристроїв відносяться апаратні ключі безпеки, смарт-картки, токени та апаратні модулі (HSM).

Апаратні ключі безпеки або токени – це невеличкі пристрої, які діють по принципу ключа від квартири чи автомобіля. Тільки відмикають вони вхід до облікового запису операційної системи або до акаунтів, що зберігаються у веб-застосунках, і на відміну від звичайних ключів, їх неможливо підробити або скопіювати. Токени здатні зберігати ідентифікаційні дані, сертифікати, ключі шифрування та іншу конфіденційну інформацію. Вони зазвичай використовуються для автентифікації, підпису документів, забезпечення безпеки та доступу до різних ресурсів.

Смарт-картки – це зазвичай пластикові картки, які містять вбудовану мікросхему з обробником, пам’яттю та інтерфейсами зв’язку. Вони можуть використовуватись для зберігання інформації, включаючи особисті дані, фінансові дані, медичну інформацію та інше. Смарт-картки часто використовуються для автентифікації, безконтактних платежів, контролю доступу, електронного паспорта та інших сфер застосування.

Основна відмінність між токенами і смарт-картками полягає у їхній формі та функціональних можливостях, проте обидва типи пристроїв використовуються для зберігання і захисту конфіденційної інформації та забезпечення безпеки в різних сферах. Проте деякі ключі безпеки мають [режим смарт-карти](https://yubikey.com.ua/rezhym-smart-kartky-yubikey-bez-dodatkovoho-obladnannia) (PIV та CCID).

Апаратний криптографічний модуль – це пристрій, що призначений для захисту криптографічних ключів (PKI) та прискорення криптографічних операцій. Він забезпечує автентичність цифрових підписів учасників мережі блокчейн та створює безпечне середовище для реалізації IT-рішень.

Криптографічні модулі існують у різних формфакторах:

PCI Express плати, що вбудовуються;

мережеві модулі;

USB-токени – найкомпактніші [пристрої для безпеки серверів](https://yubikey.com.ua/yubihsm2).

Так, на практиці для вибору найнадійніших технологічних варіантів захисту слід звертати увагу на наступні характеристики таких ключів:

сертифікацію ключів;

швидкість роботи;

можливості пристроїв;

енергоспоживання;

стійкість до зламу;

фізичну надійність;

зручність використання.

В свою чергу, апаратно-програмні засоби можна розподілити на наступні групи:

Системи ідентифікації і аутентифікації користувачів.

Такі системи застосовуються для обмеження доступу випадкових і незаконних користувачів до ресурсів комп’ютерної системи. Загальний алгоритм роботи цих систем полягає у тому, щоб отримати від користувача інформацію, яка підтверджує його особистість, перевірити її достовірність, після чого надати (чи не надати) цьому користувачу можливість роботи із системою. Під час побудови таких систем виникає проблема вибору інформації, на основі якої виконується процедура ідентифікації користувача. У загальному можна виділити наступні типи:

* + таємна інформація, якою володіє користувач (пароль, персональний ідентифікатор, ключ тощо). Цю інформацію користувач повинен запам’ятати або можуть бути застосовані спеціальні засоби зберігання такої інформації;
	+ фізіологічні параметри людини (відбитки пальців рук, малюнок райдужної оболонки ока тощо чи особливості поведінки людини (наприклад, особливості роботи на клавіатурі).
	+ Системи ідентифікації першого типу прийнято рахувати традиційними. Системи ідентифікації другого типу називають *біометричними*.

Системи шифрування дискових даних.

Основне завдання таких систем полягає забезпечення захисту від несанкціонованого використання даних, які знаходяться на носіях інформації.

Забезпечення конфіденційності даних забезпечується шляхом їх шифрування з використанням симетричних алгоритмів шифрування. Основною класифікаційною ознакою для комплексів шифрування служить рівень їх впровадження у комп’ютерну систему.

Робота прикладних програм з дисковим накопичувачем складається з двох етапів – *логічного* і *фізичного*.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому етапі основним об’єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи і апаратури. У якості об’єктів цього рівня виступають структури фізичної організації даних , наприклад, сектори жорсткого диску.

В результаті системи шифрування даних можуть здійснюватися криптографічні перетворення даних на рівні файлів (захищаються окремі файли) і на рівні дисків (захищається диск повністю).

До програм першого типу можна віднести програму-архіватор rar, до другого типу можна віднести програму шифрування Diskreet.

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяють на два класи:

* + системи *прозорого* шифрування;
	+ системи, які спеціально викликаються для виконання шифрування.

У системах прозорого шифрування криптографічні перетворення проводяться у режимі реального часу, непомітно для користувача. Наприклад, користувач записує підготовлений текстовий документ на диск, а система захисту у процесі запису проводить його шифрування.

Системи другого класу, як правило, представляють собою утиліти, які необхідно спеціально викликати, які необхідно спеціально викликати для виконання шифрування. До них наприклад відносяться архіватори зі вбудованими засобами парольного захисту.

Системи шифрування даних, що передаються по комп’ютерних мережах.

Розрізняють два основних способи такого шифрування: *канальне* шифрування і *кінцеве (абонентське)* шифрування.

У випадку канального шифрування захищається уся інформація, яка передається каналами зв’язку, включаючи службову. Процедура такого шифрування реалізується за допомогою протоколу канального рівня. Цей спосіб шифрування має наступну перевагу – вбудовування процедури шифрування на канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи.

Однак у даного методу є суттєві недоліки:

* + шифруванню на даному рівні підлягає уся інформація, включаючи службові дані транспортних протоколів. Це ускладнює механізм маршрутизації мережевих пакетів і потребує розшифрування даних в пристроях проміжної комутації (шлюзах, ретрансляторах тощо);
	+ шифрування службової інформації може призвести до появи статистичних закономірностей у шифруванні даних. що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів.

*Кінцеве (абонентське)* шифрування дозволяє забезпечити конфіденційність даних, що передаються між об’єктами (абонентами). Кінцеве шифрування реалізується за допомогою відповідного прикладного протоколу. У цьому випадку захищеним залишається лише повідомлення , а уся службова інформація залишається відкритою.

Системи аутентифікації електронних даних.

Під час обміну даними по мережах виникає проблема аутентифікації автора документа і самого документа, тобто встановлення особистості автора і перевірка відсутності змін у документі.

Для аутентифікації електронних даних застосовують код аутетифікації повідомлення (імітовставку) або електронний цифровий підпис. Під час формування коду коду аутентифікації повідомлення і електронного цифрового підпису використовують різні типи систем шифрування.

Код аутентифікації повідомлення формують за допомогою симетричних систем шифрування даних. Імітовставка виробляється з відкритих даних за допомогою спеціального перетворення з використанням секретного ключа і передається по каналу зв’язку у кінці зашифрованих даних. Імітовставка перевіряється отримувачем повідомлення, що має секретний ключ, шляхом повторення процедури, що виконувалась попередньо відправником, на отриманими відкритими даними.

Електронний цифровий підпис представляє собою відносно невелику кількість додаткової аутентифікаційної цифрової інформації, що передається разом із текстом. Для реалізації електронного цифрового підпису використовують принципи асиметричного шифрування.

Засоби управління ключовою інформацією.

Під ключовою інформацією розуміють сукупність усіх криптографічних ключів, що використовуються в інформаційній системі.

Основним класифікатором засобів управління ключовою інформацією є вид функції управління ключами. Розрізняють наступні основні види функцій управління ключами: генерація ключів, зберігання ключів і розподіл ключів.

Способи генерації ключів розрізняють для симетричних і асиметричних криптосистем. Для генерації ключів симетричних криптосистем використовуються апаратні і програмні засоби генерації випадкових чисел, зокрема схеми із застосуванням блочного симетричного алгоритму шифрування. Генерація ключів для асиметричних криптосистем являє складніше завдання у зв’язку із необхідністю отримання ключів з певними математичними властивостями.

Функція зберігання ключів передбачає організацію безпечного зберігання, обліку і видалення ключів. Для забезпечення безпечного зберігання і передачі ключів застосовують їх шифрування за допомогою інших ключів. Такий підхід призводить до концепції ієрархії ключів. До ієрархії ключів, як правило входить головний ключ (майстер ключ), ключ шифрування ключів і ключ шифрування даних. Необхідно зазначити, що генерація і зберігання ключів є критичними питаннями криптографічного захисту.

Розподіл ключів є самим відповідальним процесом в управлінні ключами. Цей процес повинен гарантувати скритність розподілу ключів, а також оперативність і точність їх розподілу. Розрізняють два основних способи розподілу ключів між користувачами комп’ютерної мережі:

* + застосування одного або декількох центрів розподілу ключів;
	+ прямий обмін сеансовими ключами між користувачами.

Системи біометричного захисту використовують унікальні для кожної людини вимірювані характеристики для перевірки особи індивіда.

Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів.

До біометричних засобів захисту інформації відносять системи аутендифікації за:

Параметрами голосу.

Візерунком райдужної оболонки ока і карта сітчатки ока.

Рисами обличчя.

Формою долоні.

Відбитками пальців.

Формою і спосібом підпису.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення.

Для того, щоб біометрична система змогла надалі аудентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Під час процедури реєстрації в базу даних системи заносяться характеристики користувачів, необхідні для встановлення їх автентичності.

Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і виносять рішення, хто постав перед сканером.

Аутентифікація по райдужній оболонці ока

Райдужна оболонка ока є унікальною для кожної людини біометричної характеристикою.

Зображення ока виділяється з зображення особи і на нього накладається спеціальна маска штрих-кодів. Результатом є матриця, індивідуальна для кожної людини.

Аутентифікація по зображенню особи

Для ідентифікації особи часто використовуються технології розпізнавання по обличчю. Розпізнавання людини відбувається на відстані. Ідентифікаційні ознаки враховують форму особи, його колір, а також колір волосся. До важливих ознак можна віднести також координати точок особи в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал).

Алгоритм функціонування системи розпізнавання: Зображення особи зчитується звичайною відеокамерою і аналізується. Програмне забезпечення порівнює введений портрет з еталоном, що зберігаються. Важливо також те, що біометричні системи цього класу здатні виконувати безперервну аутентифікацію користувача комп'ютера протягом всього сеансу його роботи

Аутентифікація по долоні руки.

У біометриці з метою ідентифікації використовується проста геометрія руки – розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин). Сканери ідентифікації по долоні руки встановлені в деяких аеропортах, банках і на атомних електростанціях.

Метод розпізнавання геометрію кисті руки заснований на аналізі тривимірного зображення кисті. Однак форма кисті руки також є параметром, який досить сильно схильний до змін в часі, а крім того, вимагає сканерів великого розміру, що веде до подорожчання системи

Аутентифікація за відбитками пальців

Оптичні сканери зчитування відбитків пальців встановлюються на ноутбуки, миші, клавіатури, флеш-диски, а також застосовуються у вигляді окремих зовнішніх пристроїв і терміналів (наприклад, в аеропортах і банках) .Якщо візерунок відбитка пальця не збігається з візерунком допущеного до інформації користувача, то доступ до інформації неможливий

Аутентифікація по характеристикам мови

Ідентифікація людини по голосу - один з традиційних способів розпізнавання, інтерес до цього методу пов'язаний і з прогнозами впровадження голосових інтерфейсів в операційні системи.

Використані джерела:

1. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.