Отже, метою створення інтелектуальних технологій є поліпшення та автоматизація рутинних справ людини. Це можливість надійного зберігання інформації в пам'яті комп'ютера, виконання певних перетворень, обчислень та надання користувачеві зручного інтерфейса програми. Сучасні фільми та серіали дають можливість нам уявити те, як виглядатиме наш світ через кілька десятків років. Адже безліч систем штучного інтелекту вже продемонстровано у таких фільмах, як «Термінатор», «Матриця», «Той, що біжить по лезу» та інші.

Незважаючи на незначні недоліки комп’ютеризованих роботів, інформаційні системи відіграють важливу роль у нашому житті. Адже кожен з нас не міг би уявити своє життя без таких речей, як «розумний» годинник, пральна машина, холодильник, мікрохвильова піч, автомобіль тощо. У наш час можна запустити усю техніку в будинку за допомогою смартфона. Сотні компаній використовують інноваційні технології для вдосконалення своєї продукції, тисячі інтелектуальних технологій застосовують для покращення стану екології та, зрештою, десятки тисяч лікарів за допомогою сучасної техніки рятують життя мільйонів пацієнтів. Технологічні винаходи будують наше майбутнє!

Список літературних джерел.

1. Стаття про робота Софію Hanson Robotics. [Електронний ресурс]. Режим доступу: https://www.hansonrobotics.com/sophia-2020/
2. Можливості Софії. Блог Hanson Robotics. [Електронний ресурс]. https://www.hansonrobotics.com/blog/
3. GitHub проект комп’ютеризованого робота Софії. [Електронний ресурс]. https://github.com/hansonrobotics

УДК 004.8

Шевчук Д. І., студент 4 курсу спеціальності 122 «Комп’ютерні науки»
Римар П. В., старший викладач кафедри інформаційних технологій

АПАРАТНІ ШИФРАТОРИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Апаратний шифратор на вигляд і по суті є звичайним комп'ютерним «залізом», найчастіше це плата розширення, що вставляється в роз'єм ISA або PCI системної плати ПК. Бувають інші варіанти, наприклад у вигляді USB-ключа з криптографічними функціями, але тут розглянуто класичний варіант – шифратор для шини PCI. Використовувати цілу плату лише для функцій шифрування – недозволена розкіш, тому виробники апаратних шифраторів

зазвичай намагаються наситити їх різними додатковими можливостями, серед яких:

- Генерація випадкових чисел
- Контроль входу комп'ютера
- Контроль цілісності файлів операційної системи

Плата з усіма наведеними можливостями називається пристроєм криптографічного захисту даних (ПКЗД). ПКЗД складається з елементів:

- Блок керування.
- Контролер системної шини ПК (наприклад, PCI).
- Енергонезалежний запам'ятовуючий пристрій (ЗП).
- Пам'ять журналу.
- Шифропроцесор (або кілька)
- Генератор випадкових чисел.
- Блок уведення ключової інформації.
- Блок комутаторів.

Шифрування в ПКЗД має виконуватися так, щоб стороннім неможливо було дізнатися ключі та якимось чином вплинути на алгоритми, що реалізуються. Іноді буває корисно засекретити правила перетворення ключів. Тому шифропроцесор логічно складається з кількох структурних одиниць:

- Обчислювач
- Блок керування
- Буфер введення-виводу

Зрозуміло будь-якому користувачеві ПК бажано, щоб присутність у його комп'ютері ПКЗД не відбивалося на зручності роботи (звісно, якщо людина виконує лише дозволені дії). Але, звичайно шифрування даних забирає деякий час, причому раніше доводилося просто чекати, коли закінчиться шифрування, наприклад, локального диска. У Windows дозволялося зайнятися чимось паралельно, але ще кілька років тому шифратори відволікали на себе значні ресурси процесора, тому без помітного гальмування можна було тільки розкладати пасьянс. Сучасні ПКЗД шифрують дані самостійно без допомоги центрального процесора ПК. У шифратор лише передається команда, а потім він сам витягує дані із ОЗУ комп'ютера, шифрує їх і кладе у вказане місце. Процесор при цьому цілком може виконувати інші завдання. Дослідження сучасних ПКЗД показують, що під час їхньої роботи продуктивність ПК практично не знижується. Можливе застосування і кількох ПКЗД на одному комп'ютері, наприклад на криптографічному маршрутизаторі: один шифрує інформацію, що надсилається в Інтернет, другий – ту ,що надходить з інтернету. Продуктивність такої системи не затримує роботу локальної мережі Fast Ethernet (100 Мбіт/с). Потокова швидкість обробки даних – це один з основних параметрів, якими оцінюють апаратні шифратори. Вона змінюється в мегабайтах за секунду і залежить насамперед від складності алгоритму шифрування.

Для захисту інформації, що передається в Мережу, можна використовувати як звичайний шифратор, так і прохідний (ПШ), який, крім усього вищепереліченого, є також повноцінним мережним адаптером Ethernet (тобто шифратор і мережевий адаптер виконані як одна PCI-плата). Його переваги в тому, що він повністю контролює весь обмін даними в мережі, а обійти його (як зсередини, так і зовні) просто неможливо.

Встановлений на комп'ютер шифратор може використовуватися відразу декількома програмами, наприклад програмою прозорого шифрування, що «проганяє» дані крізь шифратор, та програмою електронного підпису, що використовує для обчислення підписи отримані від шифратора випадкові числа. Для того, щоб не виникало колізій при одночасному зверненні до шифратора різних програм (уявимо, що одна з них шифрує логічний диск, а друга на іншому ключі розшифровує файл: якщо не керувати чергою виконання шифратором їх вимог, вийде абракадабра), ставлять спеціальне програмне забезпечення управління ними. Таке ПЗ видає команди через драйвер шифратора і передає останньому дані, стежачи за тим, щоб потоки інформації від різних джерел не перетиналися, а також за тим, щоб у шифратор завжди знаходилися потрібні ключі. Таким чином УКЗД виконує два принципово різні види команд:

- Перед завантаженням операційної системи – команди, зашиті на згадку про шифратор. Вони здійснюють всі необхідні перевірки та встановлюють необхідний рівень безпеки – припустимо, відключають зовнішні пристрої.
- Після завантаження, наприклад, Windows — команди, які надходять через модуль керування шифраторами: шифрувати дані, перезавантажувати ключі, обчислювати випадкові числа тощо.

Такий поділ необхідний з міркувань безпеки – після виконання команд першого блоку, які не можна оминути, зловмисник уже не зможе зробити щось заборонене. Ще одне призначення ПЗ управління шифраторами –забезпечити можливість заміни одного шифратора на інший (скажімо більш «просунутий» або швидкий), не змінюючи програмного забезпечення. Це відбувається аналогічно, наприклад, зміні мережної карти: шифратор поставляється разом із драйвером, який дозволяє програмам виконувати стандартний набір функцій. Ті ж програми шифрування і не помітять такої заміни, але працюватимуть у кілька разів швидше. Так само можна замінити апаратний шифратор на програмний. Для цього програмний шифратор виконують зазвичай у вигляді драйвера, що надає той самий набір функцій. Втім, таке ПЗ потрібно не всім шифраторам - зокрема, ПШ, що стоїть по дорозі до HDD, достатньо налаштувати один раз, після чого про нього можна просто забути.

Список літературних джерел.

1. Mustafa Khairallah, Hardware Oriented Authenticated Encryption Based on Tweakable Block Ciphers, 2021. 210 p.

2. Roger R. Dube, Hardware-based Computer Security Technicas to Defeat Hackers: From Biometrics to Quantum Cryptography, 2021. 205 p.
3. Luther Martin, Introduction to Identity-Based Encryption (Information Security and Privacy Series), 2008. 245 p.

УДК 004.8

Ярош О.Л., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н.А., к.е.н, доцент, доцент кафедри інформаційних технологій

ЗАХИСТ ОСОБИСТИХ ДАНИХ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Донецький Національний університет імені В. Стуса, м. Вінниця

На сьогоднішній день збір та обробка даних знайшли широке використання в найрізноманітніших сферах. Їх обробка не тільки допомагає в виконанні повсякдених задач, але й може слугувати інструментом порушення права на приватність людини. У зв'язку з цим одним із найбільш актуальних завдань є розробка систем захисту персональних даних. Створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в тому числі пов'язаних із європейською інтеграцією нашої держави. Зокрема, саме від виконання цього зобов'язання значною мірою залежать євроінтеграційні прагнення української держави.

Проблема, як виток персональних даних громадян України із автоматизованих систем державних органів та приватних компаній стає пріоритетом діяльності злочинів. Ситуація стає все більш складнішою, оскільки з'являються нові форми приховування злочинцями не лише своїх комунікацій (в т.ч. із використанням можливостей Darknet та Deepweb), але й інструментів виведення коштів (кріптовалюти).

На сьогоднішній день органи державної влади стикаються із низкою загроз та викликами в сфері кібербезпеки. В Україні існує понад 100 державних та єдиних реєстрів, які містять конфіденційну інформацію. Більшість з них використовує авторизацію за допомогою логіну та паролю, що в свою чергу має певні вразливості. Зокрема, у такий спосіб не можливо достовірно ідентифікувати особу, яка отримує інформацію з реєстру [2].

В сучасних умовах гостро стоїть проблема із захистом інформації, яка зберігається у розпорядників (держателів) реєстрів. Здебільшого мережева інфраструктура має застаріле та вразливе програмне забезпечення. Переважно користувачі, а деколи і адміністратори поряд з доступом до реєстрів мають