УДК 004.056.5

Ю.І. ГОРБЕНКО, В. А. ПОНОМАР

АНАЛІЗ АТАК З ФІЗИЧНИМ ДОСТУПОМ ТА ОБҐРУНТУВАННЯ ВИМОГ ДО ЗАХИСТУ КРИПТОГРАФІЧНИХ МОДУЛІВ ВІД НИХ

Вступ

В області інформаційних технологій все зростаючою є необхідність використання криптографічних механізмів, таких як захист даних від несанкціонованого розкриття чи маніпуляції, для аутентифікації об'єктів і неспростовності. Безпека та надійність таких механізмів безпосередньо залежить від засобів криптографічного захисту інформації (КЗІ), які реалізують дані послуги. Більшість таких засобів реалізовано у вигляді криптографічних модулів. Криптографічний модуль – це набір апаратного забезпечення, програмного забезпечення або програмно-апаратного забезпечення, який реалізує функції безпеки і міститься в межах криптографічної границі.

Захист засобу КЗІ зумовлений необхідністю забезпечення безпеки критичних параметрів. Критичні параметри безпеки (CSP) – це інформація, що пов'язана із забезпеченням функціонування криптомодуля, розкриття або зміна якої може скомпрометувати безпеку криптографічного модуля. Ключові дані теж відносять до критичної інформації.

Криптографічні модулі під час своєї роботи використовують затверджені криптографічні алгоритми, стійкість яких вже доведена. Але виникає питання про захист CSP від зловмисника, який має фізичний доступ до криптографічного модуля. Протягом часу виникали різноманітні атаки на криптомодулі з використанням фізичного доступу до них. У відповідь розробники були вимушені знаходити та реалізовувати способи протидії на ці атаки, але чим складніше становився криптомодуль (чим більше становився його функціонал), тим складніше становилося забезпечення 100 % захисту від атак з фізичним доступом до криптографічного модуля. Що стосується вимог до фізичного захисту криптографічних модулів, то існують стандарти, які їх описують – FIPS-140-3, ISO/IEC 19790:2012 [1, 2].

Класифікація атак з фізичним доступом до криптографічного модуля

Частіше за все засоби КЗІ призначені для виконання послуг конфіденційності, цілісності, автентифікації та управління доступу. Для реалізації цих послуг використовується певний набір криптографічних перетворень, для забезпечення більшого ступеня захищеності ці перетворення виконуються на основі певних секретних даних, так званих ключових даних. І саме для виконання операцій з цими даними так, щоб запобігти їх витоку, і використовуються криптографічні модулі.

Модулі в загальному випадку складаються з власне модуля (блоки пам’яті, в яких зберігається необхідна інформація та алгоритм виконання операцій), інтерфейсу, через який модуль під’єднується до персонального комп’ютера та корпуса.

Фізичний захист засобів КЗІ стосується усіх видів криптографічних модулів, крім програмного. Наведені засоби використовуються в сферах управління ключами та забезпечення конфіденційності та цілісності інформації. Найбільш частіше криптографічні модулі даного типу використовуються в побудові центру сертифікації ключів, захисті інформації в IP-мережах (на додаток до них тоді використовуються ще й шлюзи захисту), захисті електронної пошти тощо.

За критерієм методи проведення атаки поділяються на пасивні та активні [3], за способом проведення – на інвазивні та неінвазивні. Інвазивні атаки вимагають відкриття корпусу модуля, щоб отримати прямий доступ до внутрішніх компонентів. Прикладом такої атаки може бути розкриття корпусу та підключення до шини даних, щоб аналізувати передачу інформації. Неінвазивні атаки використовують інформацію, що доступна ззовні, поява чи

випромінювання якої може не передбачатися розробником: час роботи, споживання електроенергії, побічне електромагнітне випромінювання.

Під час виконання активних атак зловмисник безпосередньо втручається у функціонування модуля, наприклад для виклику помилок обчислення. Пасивні атаки виконують лише спостереження за роботою криптографічного модуля.

Атаки з фізичним доступом можуть використовуватися як самі по собі, так і як допоміжний засіб під час виконання іншої атаки (наприклад для збирання статистичної інформації для диференційного криптографічного аналізу).

Аналіз атак з фізичним доступом

1. Фізичне зчитування ключа. Зловмисник отримує прямий доступ до місця зберігання ключа та за допомогою спеціальних індикаторів фізичних полів зчитує його.

2. Атака зондуванням. Пасивна проста атака. Для отримання інформації модуль відкривається, за допомогою оптичного мікроскопа, вивчається печатна плата і встановлюються щупи на провідники, якими йдуть сигнали, або за допомогою мікроскопа досліджується стан блоків пам'яті. Процес спрощується при використанні зондувального приладу, який включає мікроскопи і мікроманіпулятори для встановлення щупів на поверхні чипа. Такі прилади використовуються в напівпровідниковій промисловості для перевірки зразків виробів. Щоб спростити спостереження криптоаналітик зазвичай уповільнює тактову частоту роботи приладу. У 2004 році Бо Янг за допомогою зондування електричних ланцюгів апаратного модуля DES – шифрування зміг відновити секретний ключ.

3. Атака за часом. Атака запропонована Полом Кохером у 1996 році [4]. Атака базується на припущенні, що різні операції виконуються в криптомодулі за різний час, залежно від поданих на вхід даних. Так, вимірюючи час обчислень і проводячи статистичний аналіз даних, можна отримати повну інформацію про секретний ключ. Принцип атаки зосереджений на отримані та аналізі дисперсії часу необхідного на виконання операцій. Вразливість до цієї атаки властива криптомодулям, які реалізують оптимізовані (швидкі) криптографічні алгоритми.

Наприклад, для алгоритму цифрового електронного підпису, що обчислюється:

$$s = \left(k^{-1}(H(m) + x * r)\right) mod\ q\ , \qquad (1)$$

де r та q відомі криптоаналітику, k^{-1} попередньо обчислений, $H(m)$ – геш-значення повідомлення, x – секретний ключ. На практиці в першу чергу обчислюється наступний вираз вираз:

$$S' = (H(m) + x * r)\ mod\ q\ , \qquad (2)$$

а потім відбувається множення на k^{-1}. Якщо використовується функція швидкого множення за модулем без витримки фіксованого часу, то час підпису буде корелюватися з часом обчислення ($x * r\ mod\ q$). Криптоаналітик може знайти час обчислення $H(m)$ і компенсувати його в загальному аналізі, що стосується додавання за модулем, то воно буде мати дуже низький вплив на загальний час. Першими у множенні за модулем використовуються найбільш значущі біти $x * r$, що залежать від відомого r та старших біт x. Таким чином, проводячи порівняння між загальним часом обчислень і своїми обчисленими еталонами, криптоаналітик зможе знайти старші біти секретного ключа, що в подальшому звузить простір ймовірних ключів чи дозволить, обчисливши нові еталони, знайти наступні біти [4].

Одним з різновидів атак за часом є також атаки на кеш, що були представлені Джоном Келсі. Цей тип атак ґрунтується на вимірюваннях часу і частоти промахів в кеші процесора і спрямований на програмні реалізації шифрів, тому на даний час цей вид атак не розповсюджений на апаратні та апаратно-програмні засоби КЗІ.

4. Атака на помилки обчислень. Активна атака, основна ідея якої полягає у здійсненні різних впливів на модуль з метою утворення викривлення інформації на деяких етапах його

роботи. Керуючи цими викривленнями і порівнюючи результати на різних етапах роботи пристрою, криптоаналітик може відновити секретний ключ. У 1997 році Ден Боне представив дану атаку на алгоритм підпису RSA та протокол ідентифікації Шнора [5]. Використання даної атаки на алгоритм блочного шифрування AES зменшує складність диференційного криптоаналізу. Вивчення атак на основі помилок обчислень зазвичай розділяються на дві групи: одна вивчає теоретичні можливості для утворення помилок в самому алгоритмі, інша – досліджує методи впливу для втілення цих помилок в конкретних пристроях. Методи впливу:

– зміна напруги живлення криптосистеми. Відхилення в живленні, що сильно перевищують задані виробником норми, можуть призвести до помилок на певних етапах роботи, не заважаючи пристрою завершити процес шифрування;

– зміна будови модуля (порушення електричних контактів);

– зміна тактової частоти криптографічного пристрою. При точному керуванні відхиленням тактової частоти від заданої норми можна досягти повної зміни виконання інструкцій в модулі, аж до невиконання певної інструкції. Такі атаки особливо поширені на смарт-карти, тактовий сигнал для яких подається зовнішнім генератором;

– вплив лазерним променем або сфокусованим світовим потоком. За допомогою такого впливу можна змінювати стан комірки пам'яті і впливати на умовні переходи у виконанні коду;

– вплив змінним магнітним полем. Змінне магнітне поле викликає в ланцюгах пристрою вихрові струми, які можуть змінювати стан комірок пам'яті;

– розташування модуля у сильному електромагнітному полі;

– підвищення температури якоїсь частини криптомодуля.

5. Атака на енергоспоживання. Пасивна атака, запропонована Полом Кохером у 1999 році [6]. Сутність цієї атака полягає в тому, що в процесі роботи модуля криптоаналітик з високим ступенем точності вимірює енергоспоживання пристрою і таким чином отримує інформацію про виконувані в пристрої дії та їх параметри. Через те, що живлення пристрою зазвичай подається ззовні, таку атаку легко втілити: достатньо послідовно приєднати в коло живлення резистор і точно вимірювати струм, що проходить крізь нього. Інший спосіб – вимірювати зміну напруги на входах і виходах криптомодуля під час роботи.

Атаки на енергоспоживання часто використовуються як підготовчий етап більш складної атаки [3, 6]. Наприклад, на рис. 1 показано енергоспоживання засобу, що виконує AES шифрування. На рисунку видно 10 однакових частин, що відповідають 10 раундам алгоритму AES, це не дає ніякої додаткової інформації, але може використовуватися в подальшому криптоаналізі.

В той самий час можлива повноцінна атака даного типу на реалізацію швидкого алгоритму підведення у степінь що використовується в RSA [3]. За даним алгоритмом, якщо біт степені не нульовий, виконується додаткове множення. На рис. 2 показано, як аналізуючи енергоспоживання під час виконання швидкого алгоритму, можна відновити біти експоненти.

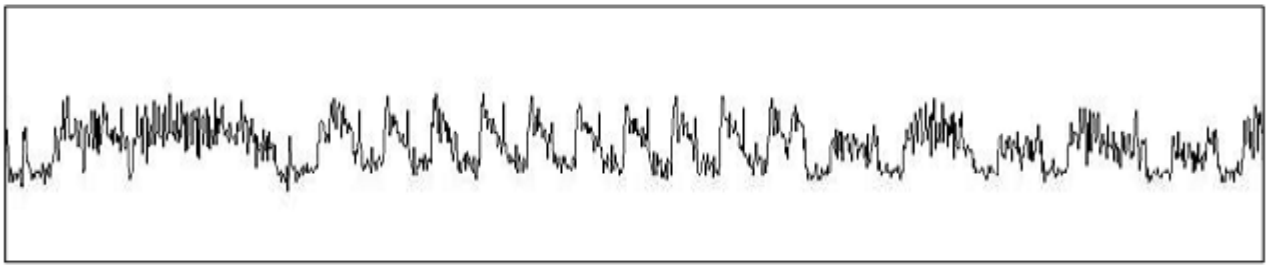

Рис. 1. Енергоспоживання криптографічного модуля під час AES шифрування

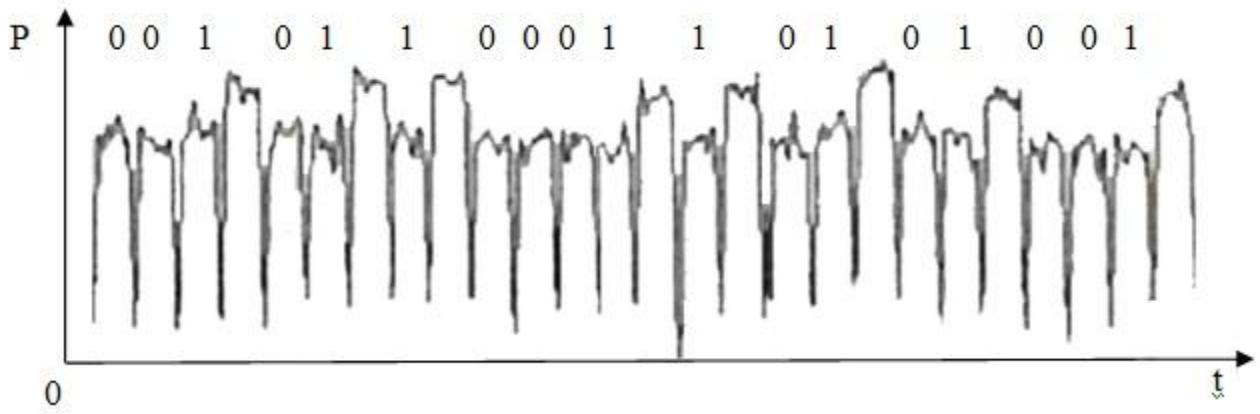

Рис. 2. Аналіз енергоспоживання в швидкому алгоритмі

6. Атаки за потужністю відрізняються високою дієвістю з точки зору затрат на криптоаналіз. Так, наприклад, проста атака за потужністю на смарт-карту здійснена за кілька секунд, а декотрі варіанти диференційних атак за потужністю дозволяють отримати секретний ключ за 15 вимірів [6].

7. Атака по електромагнітному випромінюванню. Пасивна атака, яка базується на тому, що електронні пристрої шифрування під час роботи утворюють електромагнітне випромінювання. Зв'язуючи певні спектральні компоненти цього випромінювання з операціями, що виконуються у модулі, можливо отримати достатньо інформації для визначення секретного ключа або інформації, що обробляється. Прикладом такої атаки є перехоплення ван Эйка, здійснене в 1986 році.

8. Акустична атака. Пасивна атака, спрямована на отримання інформації зі звуків, створюваних пристроєм. Історично тип таких атак пов'язується з прослуховуванням принтерів і клавіатур, але в останні роки знайшли вразливості, що дозволяють використовувати акустичні атаки на внутрішні складові шифраторів.

Зазвичай атаки за часом, на енергоспоживання та по електромагнітному випромінюванню використовуються разом. Частина використовується для звичайного збору даних, а потім за допомогою цих даних виконується спеціальна атака на даний алгоритм чи загальний диференційний криптоаналіз.

Способи протидії атакам з фізичним доступом

1. Зберігати критичні дані у зашифрованому вигляді.

2. Реалізувати систему виявлення та реагування на вторгнення, яка при виявленні фізичного доступа до печатної плати унеможливлює отримання результатів криптоаналітиком (видаляє критичні дані, блокує роботу криптографічного модуля). Система виявлення повинна реагувати на відчинення кришок або дверей корпусу, порушення його цілісності, різку зміну температури або тиску, чи ступеню зміни температури або тиску.

3. Екранування. Досить потужне фізичне екранування модуля дозволяє усунути майже всі побічні канали витоку інформації. Вадою екранування є істотне збільшення вартості і розмірів пристрою.

4. Додавання шуму. Додавання шуму істотно ускладнює задачу криптоаналітика. Шуми зменшують відсоток корисної інформації в побічному каналі, роблячи її використання недоцільним через витрати або й взагалі неможливим. Шум можливо додати як програмно (додання випадкових обчислень), так і апаратно (встановлення різних генераторів шуму). Крім того, даний захист можливо застосовувати проти акустичної атаки.

5. Вирівнювання часу виконання операцій. Щоб криптоаналітик не міг провести атаку за часом виконання, всі етапи шифрування в пристрої мають виконуватись за однаковий час. Досягти цього можна такими способами:

– додавання фіксованої затримки. Якщо відома кінцева апаратна платформа, то можна розрахувати час виконання кожної операції і вирівняти їх, додав фіксовані затримання;

– одночасне виконання декількох можливих операцій. Якщо в якийсь момент алгоритму має виконуватись або множення, або возведення у квадрат, то треба виконати обидві операції, а непотрібний результат відкинути.

6. Очевидною вадою такого підходу є уповільнення роботи модуля. Також такі заходи не допомагають від динамічних затримок, таких як промах кешу.

7. Зрівноважування енергоспоживання. Якщо можливо, при виконанні операцій треба задіяти всі апаратні частини пристрою (наприклад, регістри або вентилі), на невикористаних складових треба проводити віртуальні обчислення. Таким чином можна досягти постійності енергоспоживання пристроєм і захиститись від атак на енергоспоживання.

8. Усунення умовних переходів. Захиститись від багатьох атак сторонніми каналами можна, усунувши в алгоритмі операції умовного переходу, що залежать від вхідних даних або секретного ключа. В ідеалі алгоритм взагалі не повинен містити операторів розгалуження і всі обчислення повинні виконуватись за допомогою елементарних побітових операцій.

9. Незалежність обчислень від даних. Якщо обчислення не залежать від вхідних даних або секретного ключа, то криптоаналітик не зможе їх отримати з інформації зі стороннього каналу. Досягти цього можна такими способами:

– маскування – спосіб, при якому до даних на вході застосовують деяку маску, проводять обчислення і зворотну корекцію маски. Тобто, при атаці сторонніми каналами криптоаналітик може отримати якесь проміжне значення, що не розкриває даних, поданих на вхід;

– виконання обчислень наосліп – підхід у криптографії, за якого пристрій надає функцію криптоперетворення, при цьому не знаючи реальних вхідних даних.

Аналіз вимог стандартів до фізичного захисту криптографічного модуля

Стандарти вимог до криптографічних модулів пропонують виділити чотири наростаючі, якісні рівні вимог безпеки, які призначені для покриття широкого спектру потенційних застосувань і середовищ [1]. Вимоги фізичної безпеки визначені для трьох різних фізичних виконань криптографічного модуля.

1. Одночипові криптографічні модулі – це фізичні виконання, у яких один чіп з інтегральною схемою (ІС) може використовуватися в якості автономного пристрою, або вбудований в корпус чи в продукт, який може бути фізично не захищеним. Прикладами одночипових криптографічних модулів є поодинокий ІС-чіп або смарт-карта з одним ІС-чіпом.

2. Багаточипові вбудовані криптографічні модулі – це фізичні виконання, у яких два або більше ІС-чіпів взаємопов'язані і вбудовані в корпус або в продукт, який може бути фізично не захищеним. Прикладами багаточипових вбудованих криптографічних модулів є адаптери і плати розширення.

3. Багаточипові автономні криптографічні модулі – це фізичні виконання, у яких два або більше ІС-чіпів взаємопов'язані і весь корпус фізично захищений. Прикладами багаточипових автономних криптографічних модулів є шифруючі маршрутизатори, безпечні радіостанції або USB-токени.

У таблиці наведено вимоги фізичної безпеки, як загальні, так і для трьох конкретних виконань для кожного із чотирьох рівнів безпеки. Вимоги фізичної безпеки, що залежать від варіанту виконання, на кожному рівні безпеки посилюють загальні вимоги для цього рівня, і залежні від виконання вимоги попереднього рівня.

Вимоги безпеки визначаються і для інтерфейсу технічного обслуговування, якщо конструкція криптографічного модуля забезпечує фізичний доступ (наприклад, для постачальника модулів або іншої уповноваженої особи).

Рівень безпеки	Загальні вимоги для всіх варіантів виконань	Одночіпові	Багаточіпові вбудовані	Багаточіпові автономні
1	Заводські компоненти. Стандартна пасивація. Процедурне або автоматичне обнуління при здійсненні доступу до інтерфейсу технічного обслуговування.	Немає додаткових вимог	Корпуси виробничого класу або знімне кришки	Корпуси виробничого класу або знімне кришки
2	Доказ вторгнення Непрозорі або напівпрозорі в межах видимого спектру. Попереджають пряме спостереження через отвори і щілини.	Покриття, що доказує вторгнення на чипі або корпусі	Герметизуючий матеріал, що доказує вторгнення, або корпус з печатками, що доказують вторгнення, або стійкі замки на дверцятах та знімних кришках.	Герметизуючий матеріал, що доказує вторгнення, або корпус з печатками, що доказують вторгнення, або стійкі замки на дверцятах та знімних кришках.
3	Схема реагування на вторгнення і обнуління. Автоматичне обнуління при здійсненні доступу через інтерфейс технічного обслуговування. Запобігання зондуванню через отвори і щілини. EFP або EFT для температури і напруги.	Жорстке покриття, що доказує вторгнення на чипі, або міцний, стійкий до видалення та проникнення корпус	Жорсткий герметизуючий матеріал, що доказує вторгнення, або міцний корпус	Жорсткий герметизуючий матеріал, що доказує вторгнення, або міцний корпус
4	Оболонка з виявленням та реагуванням на вторгнення. EFP для температури та напруги. Захист від індукції помилки	Жорстке стійке до видалення покриття на чипі	Оболонка з виявленням та реагуванням на вторгнення та з можливістю обнуління	Оболонка з виявленням та реагуванням на вторгнення та з можливістю обнуління

Механізми виявлення вторгнення та реагування на вторгнення не замінюють доказ вторгнення. Криптографічний модуль повинен містити можливість реагування на вторгнення і обнуління, постійно стежити за оболонкою, що виявляє вторгнення, і, при виявленні вторгнення, відразу обнулити всі незахищені критичні дані.

Загалом, рівень безпеки 1 забезпечує базовий набір вимог. Рівень безпеки 2 додатково вимагає механізмів, що доводять вторгнення, та неможливість зібрати інформацію про внутрішні операції критичних областей модуля (непрозорість). Рівень безпеки 3 додає вимоги використання міцних або жорстких конформних або неконформних корпусів з механізмами виявлення і реагування на вторгнення на знімних кришках і дверцятах, і стійкості до прямого зондування через отвори і точки входу. На рівні безпеки 3 вимагається захист від помилок, викликаних середовищем (EFP), або тестування на помилки, що викликані середовищем (EFT). Рівень безпеки 4 додає вимоги використання міцних або жорстких конформних або неконформних корпусів з механізмами виявлення і реагування на вторгнення для всього корпусу або завдання значної шкоди модулю при вторгненні. На рівні безпеки 4 вимагається наявність захисту від EFP і захисту від атак шляхом індукції помилки.

Для рівнів безпеки 1 і 2 модуль не повинен використовувати функції захисту від EFP або проходження тестування EFT. На рівні безпеки 3 модуль повинен або використовувати функції захисту від EFP, або проходити тестування EFT. На рівні безпеки 4 модуль повинен використовувати функції захисту від EFP.

Криптографічний модуль повинен вести спостереження і правильно реагувати, коли робоча температура і напруга виходять за межі визначеного нормального робочого діапазону.

Якщо температура або напруга виходять за межі нормального робочого діапазону криптографічного модуля, механізм захисту повинен або виключити модуль, щоб запобігти подальшій експлуатації, або відразу обнулити всі незахищені критичні дані.

Вимоги до механізму обнуління

Модуль повинен надавати методи для обнуління всіх незахищених чутливих параметрів безпеки (SSP) і ключових компонентів всередині модуля. Чутливі параметри безпеки – це сукупність критичних та відкритих параметрів безпеки. Відмінність відкритих параметрів від чутливих полягає в тому, що відкриті параметри не потрібно захищати від витоку, а необхідно лише забезпечувати їх цілісність та доступність.

Управління SSP охоплює генератори випадкових біт (RBG), генерацію SSP, встановлення SSP, введення/виведення SSP, зберігання SSP та обнуління незахищених SSP.

В якості зашифрованих розглядаються CSP, які зашифровані з використанням затвердженої функції безпеки. CSP, зашифровані або скриті з використанням незатверджених функцій безпеки, в рамках даного міжнародного стандарту вважаються незахищеними, у вигляді відкритого тексту.

CSP в межах модуля повинні бути захищені від несанкціонованого доступу, використання, розкриття, зміни і заміни.

Хеш-значення паролів, інформація про стан RBG і проміжні значення генерації ключа повинні розглядатися як захищені CSP.

Якщо затверджені функції безпеки, методи генерації SSP або встановлення SSP вимагають випадкових значень, то для надання цих значень повинні використовуватись затверджені RBG.

Для рівнів безпеки 1 і 2 CSP у вигляді відкритого тексту, ключові компоненти і дані автентифікації можуть бути введені і виведені через фізичний порт і логічний інтерфейс, поєднані з іншими фізичними портами і логічними інтерфейсами криптографічних модулів.

На додаток до рівнів безпеки 1 і 2, для рівня безпеки 3 CSP, ключові компоненти і дані автентифікації повинні вводитися і виводитися з модуля або в зашифрованій формі, або через довірений канал.

CSP, що є секретними або особистими криптографічними ключами у вигляді відкритого тексту, повинні вводитися або виводитися з модуля, використовуючи процедуру розподілу знань і з використанням довіреного каналу.

Якщо модуль використовує процедуру розподілу знань, модуль повинен реалізовувати окремі процедури особистісної автентифікації оператора для введення або виведення кожного ключового компонента, і, принаймні, два ключові компоненти повинні знадобитися, щоб відновити оригінал криптографічного ключа.

На додаток до рівня безпеки 3, для рівня безпеки 4 модуль повинен використовувати окремі процедури багатофакторної особистісної автентифікації оператора для введення або виведення кожного ключового компонента.

Тимчасово збережені SSP та інші збережені значення, що належать модулю, повинні бути обнулені, якщо вони більше не знадобляться в майбутньому чи при загрозі витоку.

Для рівня безпеки 1 обнуління незахищених SSP може бути виконане процедурно оператором модуля, без керування модулем (наприклад, переформатування жорсткого диска, атмосферне руйнування модуля при повторному введенні і т.д.).

Для рівнів безпеки 2 і 3 криптографічний модуль повинен виконувати обнуління незахищених SSP (наприклад, шляхом перезапису нулями або одиницями або випадковими даними). Обнуління повинне виключати можливість перезапису незахищених SSP іншими незахищеними SSP. Тимчасові SSP повинні бути обнулені, коли вони більше не потрібні. Модуль повинен надавати індикацію статусу, коли обнуління завершене.

На додаток до вимог рівнів безпеки 2 і 3, для рівня безпеки 4 пред'являються наступні вимоги:

− обнуління повинне бути негайним і безперебійним і здійснюватися за досить малий період часу, щоб запобігти відновленню критичних (чутливих) даних в час між початком обнуління і фактичним завершенням обнуління;

− всі незахищені SSP, і у відкритій формі, і криптографічно захищені, повинні обнулятися так, щоб модуль повертався в заводський стан.

Висновки

Використання засобів КЗІ для надання послуг безпеки є невід'ємною частиною сучасного захисту інформації. Тому аналіз вимог до криптографічних модулів є одним з необхідних напрямків їх дослідження, бо вибір необхідного засобу КЗІ виконується методом знаходження відповідності між вимогами, що визначаються моделлю загроз, та вимогами, що виконуються криптографічним модулем.

Існує велика кількість різноманітних атак, спрямованих на застосування фізичного доступу до засобу криптографічного захисту інформації. З розвитком технологій їх кількість збільшується, і виникає необхідність в захисті криптографічних модулів від таких атак.

Більшість атак є складовими частинами комбінованої атаки на засіб КЗІ. Але деякі з них є самодостатніми атаками, що базуються на вразливостях чи недоліках криптографічних алгоритмів та будови криптомодуля. Крім того, самодостатніми є атаки, що використовують побічний канал витоку інформації та побудовані на принципах диференційного криптоаналізу.

Існуючі стандарти передбачають можливість застосування даних атак криптоаналітиком і висувають вимоги до реалізації захисту від них.

Список літератури: 1. *ISO/IEC 19790 : 2012*. Information technology – Security techniques – Security requirements for cryptographic modules. – International standard, Geneva, 2012. – 72p. 2. *Terryn W*. Fips 140-3. – International Book Marketing Service Limited, 2011. – 76p. 3. *Standaert, F.-X*. Introduction to Side-Channel Attacks / F.-X. Standaert // Secure Integrated Circuits and Systems. – 2009. – P. 27 – 44. 4. *Kocher, P*. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems / P. Kocher // Computer Science. – Santa-Barbara, California, USA, 1996. – vol 1109. – P. 104 – 113. 5. *Boneh, D. DeMillo, R. A. Lipton, R. J*. On the importance of checking cryptographic protocols for faults. / D. Boneh, R. A. DeMillo, R. J. Lipton. // EUROCRYPT '97. – 1997. – LNCS 1233. – P. 37 – 51. 6. *Kocher, P. Jaffe, J. Jun, B*. Differential Power Analysis / P. Kocher, J. Jaffe, B. Jun // Computer Science. – Santa-Barbara, California, USA, 1999. – vol 1666. – P. 398 – 412.

Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 12.03.2015