УДК 004.056.51

О.А. ШЕВЧУК, Ю.І. ГОРБЕНКО, канд. техн. наук

АВТЕНТИФІКАЦІЯ АПАРАТНИХ ЗАСОБІВ КЗІ

Розвиток ринку засобів криптографічного захисту інформації (КЗІ) надає актуальності як новим задачам, так і стимулює розвиток підходів до існуючих, таких як задача побудування моделей порушника та загроз. Зростання числа сторін, що беруть участь у виробництві засобів КЗІ, поставці, інсталяції, супроводженні в експлуатації, використанні тощо, вимагає додаткового аналізу вразливостей компонент системи в змінених умовах [7].

В [1] було розглянуто вразливість схем ЕЦП, що ґрунтуються на перетвореннях в групі точок еліптичної кривої, до зловживань з боку виробника.

Метою статті є аналіз впливу визначеної загрози з врахуванням деякої третьої сторони, що може бути задіяна в процесі розповсюдження апаратних засобів, а також розробка рекомендацій.

Огляд існуючих вимог та рекомендацій до апаратних засобів КЗІ

В світових стандартах та рекомендаціях [4, 5] існує ряд вимог щодо виконання процесів на усіх етапах життєвого циклу криптографічних засобів. Розглянемо узагальнене тлумачення можливостей порушника з урахуванням виконання визначених процедур:

- порушника відокремлено від процесу розробки та створення засобу КЗІ;
- порушник в певній мірі має фізичний доступу до засобу КЗІ ще до закінченя процесу інтеграції та безпосереднього використання засобу користувачем;
- компрометація ключової інформації за рахунок прямого доступу до елементів збереження ключової інформації неможлива, так як засіб КЗІ ще не пройшов етапу персоналізації;
- компрометація ключової інформації або ключів сесій та векторів ініціалізації за рахунок аналізу показників електромагінтного випромінювання, живлення та інших фізичних каналів витоку не має сенсу, так як засіб КЗІ ще не пройшов етапу персоналізації.
- не існує можливість зміни криптографічних алгоритмів за рахунок прямого доступу до елементів збереження алгоритмів перетворень або фізичної модифікації пристрою.

Також будемо вважати, що [1, 4]:

- порушника відокремлено від процесу та середовища використання засобу КЗІ;
- порушник не може перехопити та втручатися у канал зв'язку з засобом;
- порушник не може використовувати фізичні канали витоку інформації для персоналізованого засобу КЗІ;
- порушник може використати результати некоректної роботи модуля, що викликані недоліками реалізації та не виявлені в процедурі самотестування, якщо вони знаходяться у відкритому доступі;
- недійсні (з помилками) результати криптографічних перетворень можуть знаходитися у відкритому доступі;
- результати криптографічних перетворень, що були отримані у помилковому стані, можуть знаходитися у відкритому доступі та призвести до компрометації ключової інформації;
- використання засобу КЗІ у відкритому середовищі не розглядається.

Введені вище моделі порушника та загроз, які він може реалізувати, дозволяють запропонувати заходи протидії загроза порушника. Проведений аналіз показав, що їх необхідно розробляти перше за все з урахуванням вимог міжнародного стандарту FIPS-140 [5] та стандарту PCI HSM [4]. Основними з них можуть бути такі:

- наявність та застосування самотестування модуля КЗІ;
- повна перевірка справжності, цілісності та автентичності даних оновлення;

- автентифікація користувача, та впровадження розподілу доступу;
- впровадження відповідного рівня забезпечення фізичної цілісності засобу КЗІ.
- контроль фізичної цілісності модуля криптографічного захисту.

Наведені рекомендації та оцінки дозволяють зробити висновок, що у випадку дотримання рекомендацій порушник не може внести не випадкові (детерміновані) зміни до засобу (модуля КЗІ). Але в [4, 5] та і наведених вище рекомендаціях не визначено, які заходи потрібно прийняти для протидії загрозам, що пов'язані з підміною засобів КЗІ. Тобто, користувач не може однозначно визначити, чи є отриманий засіб КЗІ саме тим виробом, з характеристиками якого він ознайомлений чи навіть закупив його. Розглянемо вразливості такої загрози, зважаючи на необхідність перекриття такої загрози, розглянемо та проведемо більш детальний аналіз загрози підміни засобу КЗІ, але за умови використання електронного цифрового підпису (ЕЦП).

Аналіз та оцінка вразливості загрози підміни засобу КЗІ

Із аналізу [1, 4] можна зробити висновок, що загроза підміни засобу КЗІ, що надає послугу ЕЦП у визначеному середовищі, може бути реалізована за таких умов:

- порушник не може модифікувати інтерфейс обміну з засобом КЗІ для компрометації ключових даних, так як він не має доступу до засобу під час та після персоналізації;
- порушник не може створити додатковий фізичний канал витоку ключової інформації;
- порушник може створити додатковий канал витоку ключової інформації з результатом обробки вхідних даних;
- порушник може ініціювати підпис довільних даних, та додати результат обчислень до дійсного результату;
- порушник може замінити процедуру випадкової генерації особистого ключа та ключів сесії на псевдовипадкову, з відомим вектором ініціалізації.

Аналіз ряду джерел та проведені дослідження [1] дозволяють уточнити умови їх реалізації та запропонувати заходи протидії. Оскільки порушник не може взаємодіяти з засобом КЗІ під час та після персоналізації модуля, то єдиним каналом обміну інформації є відкриті документи, що з використанням відповідного засобу КЗІ.

Далі, для захисту програмного засобу КЗІ від загрози підміни необхідно та достатньо забезпечити цілісність та автентичність програмного забезпечення, що використовується. Дійсно, нехай існує програмна реалізація криптографічного алгоритму $S(k,m)$, що представлена у вигляді повідомлення $M_{S(k,m)}$, та його цифрового підпису $S(k,M_{S(k,m)})$. Нехай також порушник може створити новий алгоритм $S'(k,m)=\alpha\cdot S(k,m)$, що відрізняється від оригінального, наприклад у вигляді повідомлення $M_{\alpha\cdot S(k,m)}$. Нехай також $S(k,M_{\alpha\cdot S(k,m)})=S(k,S(k,m))$. Тоді $M_{\alpha\cdot S(k,m)}=M_{S(k,m)}$, та відповідно $\alpha\cdot S(k,m)=S(k,m)$. Тоді $\forall k\in K, m\in M:\alpha\cdot S(k,m)=S(k,m)$. Але $\alpha\cdot S(k,m)\neq S(k,m)$.

Далі, у разі виконання засобу КЗІ як програмно-апаратного засобу, або апаратного, користувач не має можливості представити алгоритм його роботи у вигляді тексту, та упевнитися у цілісності та автентичності алгоритмів, що реалізує засіб.

Дійсно, для дослідження справжнього алгоритму, за яким виконує обчислення апаратний засіб, необхідна фізична декомпозиція корпусу захисту засобу та його внутрішніх компонентів, що призведе до припинення функціонування пристрою.

Розглянемо випадок, коли відсутнє засвідчення справжності(дійсності) засобу КЗІ, що надає послуги ЕЦП в визначеному середовищі. Для міжнародних стандартів цифрових підписів, в тому числі і українського стандарту ДСТУ 4145:2002, використовуються такі елементи, що формуються випадковим чином:

- сеансовий ключ;
- особистий ключ.

До них висуваються такі вимоги:

- випадковість.
- контроль цілісності;
- конфіденційність;
- непередбачуваність;
- необоротність.

Проведемо аналіз можливих впливів порушника на забезпечення визначених вимог та наслідки цього впливу. По-перше, особистий ключ X_a обчислюється за допомогою деякої випадкової функції $\mathrm{RNG}()$. Властивості, алгоритми та вимоги до випадкової функції $\mathrm{RNG}()$, що використовуються під час процесу генерації ключових даних, визначено стандартами FIPS 186-3, NIST SP 800-50 та іншими. Особистий ключ обчислюється під час персоналізації пристрою, та у разі необхідності, в тому числі в процесі використання. Але порушник може виконати деяку модифікацію псевдовипадкової функції, як $\alpha \cdot \mathrm{RNG}()$, для зміни властивості непередбачуваності, але із зберіганням властивості випадковості, наприклад утворюючи генератор псевдовипадкових послідовностей з відомим проміжком стартових значень $log_2 \#\{s_1, s_2, \ldots s_n\} < \Theta$.

У цьому випадку на етапі персоналізації значення особистого ключа користувача засобу КЗІ набуде таких значень, що порушник може обчислити його за поліноміальний час. Далі, за наявності послуг імпорту та експорту ключових даних, користувач може генерувати ключ на довіреному засобі, та завантажити його в засіб. В такий спосіб користувач може контролювати проходження персоналізації.

Подальший розгляд пов'язаний з аналізом можливих варіантів персоналізації криптографічного засобу, що модифікований визначеним шляхом. Нехай порушник виконав підмінений (компрометований) апаратний засіб таким чином, що в в процесі персоналізації використовується ключ, який може бути обчислений порушником за поліноміальний час. Нехай також користувач створює деякий и особистий ключ X_a, та відповідний йому відкритий ключ P_a за допомогою уже компрометованого засобу. Тоді, $X_a = \alpha \cdot RNG()$, та відповідний йому відкритий ключ $P_a = GenPubKey(X_a, \ldots)$, де $GenPubKey$ – деяка функція обчислення відкритого ключа. Користувач за допомогою засобу обчислює деякий цифровий підпис $Sign(X_a, m)$, та, не використовуючи, засіб перевіряє цифровий підпис $Verify(P_a, Sign(X_a, m))$. Підпис буде дійсним, так як він відповідає відкритому ключу P_a, а його було створено за допомогою засобу уже компрометовного ключа X_a.

Далі, нехай порушник використав підмінений (компрометований) апаратний засіб таким чином, що в в процесі персоналізації використовується ключ, який може бути обчислений порушником за поліноміальний час. Нехай також користувач завантажує деякий особистий ключ X_a, та відповідний йому відкритий ключ P_a, якого було отримано за стороннім довіреним генератором. За такої умови ключ X_a відповідає вимогам, та є непередбачуваним для порушника. Нехай апаратний засіб обчислює деякий компрометований особистий ключ $\alpha(X_a)$ та користувач за допомогою засобу КЗІ обчислює деякий цифровий підпис $\mathrm{Sign}(X_a, m)$. Далі користувач, не застосовуючи засіб КЗІ, перевіряє цифровий підпис $\mathrm{Verify}(P_a, \mathrm{Sign}(X_a, m))$. Якщо $\alpha(X_a) = X_a$, тоді перевірка дійсна, причому особистий ключ відповідає тому, що було завантажено користувачем. В іншому випадку користувач констатує факт компрометації ключа.

В той же час порушник може використати особливості алгоритмів ЕЦП для компрометації особистого ключа, який було отримано за довіреним каналом, та завантажено у компрометовний пристрій.

Наведена в [1] вразливість дозволяє порушнику компрометувати особистий ключ із наступними загальними характеристиками:

• за відношенням до АС – зовнішній;
• за місцем дії – з відсутнім доступом до контрольованої зони;
• за часом дії – до персоналізації засобу КЗІ;
• за рівнем та можливостями: порушник I-II рівня, з можливістю замовити розробку засобу КЗІ за власним технічним завданням
• порушнику відома загальна структура, функції та алгоритми взаємодії з засобом КЗІ.

Як було позначено, у діючих міжнародних нормативних документах не виділяють цей клас атак, але в вимогах до апаратних засобів КЗІ, що визначені в Payment Card Industry (PCI), сформовані адміністративні вимоги, виконання яких спрямовано на запобігання реалізації визначених загроз.

В процесі досліджень встановлено, що специфікація PCI HSM 1.0 від 2009 р. [8] визначає основоположні адміністративні вимоги до створення та транспортування засобів КЗІ через сітку дистрибуції.

Сутність вимог зводиться до наступного:

• дизайн криптографічного засобу має захищати пристрій від підміни таким чином, щоб створення подібного було економічно невигідно;
• якщо криптографічний засіб має бути автентифіковано, в розумінні наявності унікального секрету пристрою, тоді цей секрет має бути унікальним для кожного криптографічного засобу, невідомий та непередбачуваний довільній особі, та завантажений до пристрою з подвійним контролем, для запобігання компрометації секрету;
• криптографічний засіб має бути доставлено до місця персоналізації за визначеним маршрутом, що передбачає аудит та контроль місце знаходження кожного пристрою в кожний проміжок часу;
• обов'язкова явна процедура передачі пристрою від виробника до особи, що здійснює персоналізацію;
• за час пересування від виробника до особи, що здійснює персоналізацію, пристрій має знаходитись у пакуванні, що дозволяє виявити неавторизований доступ до пристрою.

Далі, в новій специфікації PCI HSM 2.0[4], що набуде сили в 2012 р., внесено ряд додаткових вимог, в тому числі:

• виробник має надавати інструкції, в тому числі в глобальній мережі, щодо перевірки користувачем цілісності та справжності засобу, якщо це неможливо, необхідно виконання умов (D1) з PCI HSM 1.0 [8];
• якщо в доставці пристрою беруть участь декілька сторін, тоді перевірка пакування та вимог є обов'язком кожної сторони;
• документація до пристрою має містити інструкції щодо автентифікації критичних компонентів системи;
• якщо засіб КЗІ персоналізується виробником, то виробник має перевірити автентичність засобу перед завантаженням;
• якщо засіб КЗІ персоналізується іншою стороною, виробник має надати можливість перевірити автентичність засобу перед персоналізацією;
• кожен засіб має мати унікальний ідентифікатор, або має бути ідентифікований криптографічним шляхом.

Необхідно зазначити, що PCI HSM [4,8] не вказує на методи забезпечення визначених вимог. На нашу думку, використання криптографічних алгоритмів та примусова автентифікація засобу користувачем на етапах персоналізації є суттєвим та невід'ємним заходом.

Проведені дослідження та отримані результати дозволяють зробити наступні висновки та рекомендації:

• засоби КЗІ, що надають послуги цифрового підпису особливо вразливі до загрози підміни.

• за умов підміни пристрою, та публікації документів з цифровим підписом в відкритих джерелах, що обчислено за допомогою засобу, порушник може компрометувати особистий ключ користувача з поліноміальною складністю;

• задача визначення наявності порушення вимог до генерації ключа сеансу є обчислювальне складною.

• проблема автентифікації засобів КЗІ визнана актуальною, що підтверджують зміни до адміністративних вимог процесів забезпечення інформаційної безпеки, зокрема PCI HSM [4, 8].

• нині не опубліковано рекомендацій та не прийнято стандартів та регламентів, що визначають протоколи та методи надання послуги автентифікації засобів КЗІ.

• на ринку криптографічних засобів України не представлено засобів, що надають послугу автентифікації;

• доцільно розробити вимоги та рекомендації щодо реалізації послуги автентифікації апаратного засобу КЗІ;

• в рамках розробки вимог необхідно визначити криптографічні методи автентифікації.

Метод автентифікації засобу криптографічного захисту інформації, вразливого до підміни

Автентифікація являє собою процес встановлення достовірності твердження, що суб'єкт або об'єкт має очікувані властивості. По суті, механізм дозволяє одній сутності перевірити визначені властивості іншої, а реалізацію механізму автентифікації можна розглядати як метод захисту користувачів та власників інформація та ресурсів від різних видів обману. Механізми автентифікації реалізуються на основі застосування криптографічних протоколів та дозволяють захистити інформацію чи ресурси від їх модифікації, підміни чи створення хибних. Аналіз показав, що механізми автентифікації та їх реалізації у вигляді криптографічних протоколів дозволяють здійснити автентифікацію джерела, в тому числі:

• перевірку цілісності джерела повідомлення;
• ідентифікацію відправника повідомлення;
• перевірку цілісності отриманих даних;
• перевірку актуальності повідомлення;
• перевірку дійсності відправника.

Відносно автентифікації сутності може здійснюватись:

• автентифікація клієнта;
• автентифікація сервера;
• автентифікація засобу взагалі;
• одностороння чи взаємна автентифікація;
• генерацію автентифікованих ключів.

Враховуючи наведене, розглянемо передумови до необхідності виконання протоколу автентифікації засобу КЗІ. Із наведеного випливає, що автентифікація пристрою зумовлена наявністю вразливостей відносно апаратних реалізацій алгоритмів ЕЦП, що засновано на схемах DSA Ніберг – Рюпеля, в першу чергу до загрози підміни. Вказане можна пояснити наступним:

• реалізація загрози на будь-якому етапі циклу використання засобу може призвести до компрометації особистого ключа користувача;

• виробник апаратного засобу є стороною, якій довіряє користувач;

• виробник гарантує якість засобу КЗІ;

• компрометація засобу не має призводити до компрометації інших засобів;

• виробник не може мати відомості щодо усіх можливих користувачів засобу, але має мати відомості про усі пристрої, що було створено;

• засіб КЗІ та виробник не мають можливості оновлювати ключову інформацію;

• користувач до персоналізації засобу може не мати можливості його використання.

У цілому, згідно з наведеною моделлю загроз, необхідно зробити висновок про необхідність односторонньої автентифікації сутності (засобу КЗІ). Це пояснюється тим, що в рамках визначеної моделі загроз, критичним до загрози підміни є проміжок часу між створенням засобу виробником та персоналізацією засобу користувачем. Таким чином, процес автентифікації пристрою не пов'язаний з процесом автентифікації та авторизації користувача пристроєм після персоналізації, та має розглядатися відокремлено. Проведений аналіз [1, 4] показав, що в указаних стандартах не наведені вимоги до автентифікації сутності, але є посилання на протоколи узгодження ключів ISO/IEC 11770-2, ISO IEC 11770-3. Комітетом міжнародної стандартизації ISO/IEC узгоджено групу стандартів ISO/IEC 9798, що містять алгоритми автентифікації та посилаються на ISO/IEC 11770-2,3. Розглянемо протокол автентифікації стандарту ISO IEC 9798-2,№6.1, що є еквівалентним протоколу №8, наведеному в ISO/IEC 11770-2.

Сутність протоколу є у наступному:

• ініціатор перевірки U відсилає третій довіреній стороні згенерований новий параметр N_u та розпізнавальний ідентифікатор D.

• третя довірена сторона V створює та відсилає об'єкту U маркер, що містить параметри новизни N_u та ключ сенсу K_{UD}, ідентифікатор D, що зашифровані загальним з V ключем K_{VU}. Також V створює та відсилає новий параметр новизни N_v, сессійний ключ K_{UD} та ідентифікатор U, що зашифровані загальним з V та D ключем K_{VD};

• об'єкт D перевіряє першу частину маркеру шляхом розшифрування його зашифрованої частини спільним ключем K_{VD} та перевіряє: дійсність параметру новизни; дійсність ідентифікатору D.

Після цього U формує та пересилає об'єкту D другу частину отриманого маркеру, створює та відсилає маркер, що зашифрований спільним ключем U та $D - K_{UD}$, випадковий параметр N_{UD} та ідентифікатор B.

• Об'єкт D, отримавши маркери, розшифровує першу частину спільним ключем K_{VD}, перевіряє дійсність ідентифікатору U та відновлює спільний секрет K_{UD}. За спільним секретом K_{UD} об'єкт D розшифровує та перевіряє дійсність ідентифікатору D у другому маркері.

• Далі D відсилає U зашифрований спільним ключем K_{UD} маркер, що містить ідентифікатор U та випадковий параметр N_{UD}.

• U розшифровує маркер спільним ключем K_{UD} та перевіряє дійсність ідентифікатору U. У разі успішного виконання автентифікація завершена.

Повний протокол:

U → V: N_U, D

V → U: $\{N_U, K_{UD}, D\}_{K_{VU}}, \{N_V, K_{UD}, U\}_{K_{VD}}$

U → D: $\{N_V, K_{UD}, U\}_{K_{VD}}, \{N_{UD}, D\}_{K_{UD}}$

D → U: $\{N_{UD}, U\}_{K_{UD}}$

U: $U^D = U^U$

Наведений вище криптографічний протокол має такі характеристики:

• для процесу автентифікації в протоколі використовується спільний для двох об'єктів

секретний ключ, що розподілено між сторонами;

• один з об'єктів дає запит третій довіреній стороні на отримання ключа K_{UD};

• новизна забезпечується протоколом використанням змінного у часі параметру N_U та розподіленим ключем K_{UD};

• сторони U та D є рівноправними, причому обидві сторони розділяють ключі K_{TU} та K_{TD} з третьою довіреною стороною;

• протокол має суттєвий недолік, так як адміністративним стандартом PCI HSM 2.0[4] визначено, що можливість перевірка автентичності пристрою має бути надана особі, що здійснює персоналізацію пристрою, а також сторонам, що виконують доставку пристрою.

Аналіз наведених характеристик дозволяє висунути до всіх сторін, що задіяні в транспортуванні, зберіганні, реалізації та персоналізації пристрою, такі вимоги:

• їм необхідно звернутися до виробника для вироблення ключів;

• оновлювати ключі у випадку компрометації, або через визначений проміжок часу.

• виробник зобов'язаний зберігати інформацію про всіх постачальників (в тому числі і проміжних) та клієнтів;

• сторони U та D мають знати про існування одна одної, що викликає істотні труднощі ще на етапі створення засобу.

Приклад розподілу секрету наведено у таблиці:

Розподіл секрету у протоколі ISO/IEC 9798-2.6.1 – (*а*) та запропонованому – (*б*)

→	**V**	**U**	**D**
V	---	√	√
U	√	---	X
D	√	X	---

а

→	**V**	**U**	**D**
V	---	X	√
U	√	---	X
D	√	X	---

б

Пропонується зробити модифікацію розподілу секрету (таблиця (*а*)), змінивши симетричні криптоперетворення для обміну таким чином:

$$1 \quad U \rightarrow V: \quad \{D, T_{UV}\}_{PK(V)}$$
$$2 \quad V \rightarrow U: \quad \{\{N_V, T_{VD}\}_{K_{VD}}, \{N_V\}_{T_{VD}}\}_{T_{UV}}$$

Удосконалений протокол має наступні властивості:

• спрощується задача зберігання секретів виробником, при цьому виробник не має турбуватися про факти компрометації секрету користувача, оновлення секрету та ідентифікацію;

• забезпечується захист від перехопленням порушником токену перевірки $\{N_V\}_{T_{VD}}\}_{T_{UV}}$.

Вказане необхідне для унеможливлення атаки за паралельними каналами, у випадку використання мережевого засобу КЗІ.

Якщо засіб КЗІ не має доступу до мережі, тоді перші кроки протоколу можуть бути спрощені наступним чином:

$$1 \quad U \rightarrow V: \quad D, N_{UV}$$
$$2 \quad V \rightarrow U: \quad \{\{N_V, T_{VD}\}_{K_{VD}}, \{N_V\}_{T_{VD}}, N_{UV}\}_{SK(V)}$$

Це можливо, так як компрометація токену не призведе до здійснення атаки паралельними каналами.

З урахуванням наведеного остаточний варіант запропонованого криптографічного протоколу автентифікації має наступний вигляд:

1	U	→	V:	$\{D, T_{UV}\}_{PK(V)\}}$
2	V	→	U:	$\{\{N_V, T_{VD}\}_{K_{VD}}, \{N_V\}_{T_{VD}}\}_{T_{UV}}$
3	U	→	D:	$\{N_V, T_{VD}\}_{K_{VD}}$
4	D	→	U:	$\{N_V\}^D_{T_{VD}}$
			U:	$\{N_V\}^D_{T_{VD}} = \{N_V\}^U_{T_{VD}}$

Висновки

При створенні засобів КЗІ та їх використанні необхідно враховувати, що для апаратних та програмних засобів КЗІ повинно розроблятися різні моделі загроз;

1. Для схем ЕЦП, що ґрунтуються на алгоритмах DSA та Ніберг – Рюпеля, існує реальна загроза повного розкриття для випадку реалізації вразливості до лінійно пов'язаних ключів сеансу.

2. Діючі світові стандарти та нормативні документи, такі як FIPS-140 та PCI HSM не відокремлюють загрозу повного розкриття через реалізацію загрози підміни. Рекомендації PCI HSM визначають тільки ряд адміністративних заходів, при виконанні яких забезпечується можливість протидії реалізації загрози підпміни, але тільки на проміжку між створенням засобу КЗІ та його персоналізацією.

3. PCI HSM визначає можливість автентифікації засобу КЗІ особою, що здійснює персоналізацію, але не визначає посилання та інші документи або методи, за якими вона має бути здійснена.

4. Запропоновані модифікація механізму та криптографічного протоколу ISO/IEC 9798-2 № 6.1. дозволяє усунути визначені недоліки.

- реалізуючи лише алгоритми симетричного шифрування у засобі КЗІ;
- забезпечуючи виконання вимог PCI HSM 2.0 щодо доставки засобів КЗІ за допомогою третіх служб без попередньої реєстрації та розподілу ключового матеріалу та обов'язкової реєстрації користувачів.

Список літератури: 1. *Шевчук, О.* Актуальність атаки на зв’язанних ключах для апаратних реалізацій засобів КЗІ // Радиотехника. – 2011. – № 166. – С. 70 – 75. 2. *Шевчук, О.* Алгоритми відновлення повідомлення ЕЦП стандарту ISO/IEC 9796-3 та екзистенціальна підробка підписів, що засновується на них // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 183-187. 3. *Gallagher, P., Foreword, D. D., Director, C. F.* FIPS PUB 186-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS). – 2009. 4. *Hardware* Security Module (HSM) v2.0. – 2012. – Secuirty Standards Council. – URL: https://www.pcisecuritystandards.org/security_standards/documents.php. 5. Terryn W. Fips 140-3. – International Book Marketing Service Limited, 2011. – URL: http://books.google.com.ua/books?id=fjBWXwAACAAJ. 6. *Gallo, R., Kawakami, H., Dahab, R.* On device identity establishment and veriication // inproceedings of the 6th European conference on Public key infrastructures, services and applications. – Pisa, Italy: Springer-Verlag, 2010. – С. 130 – 145. – (EuroPKI’09). – URL: http://dl.acm.org/citation.cfm?id=1927830.1927843.0 7. FIPS 140-1 and FIPS 140-2 Vendor List. – URL:http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm. 8. Hardware Security Module (HSM) v1.0. – 2009. – Secuirty Standards Council. – URL:https://www. Pcisecuritystandards.org/documents/PCI HSM Security Requirements v1.0 final.pdf.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 17.09.2012