УДК 538.3+537.86

АНАЛІЗ ТА УДОСКОНАЛЕННЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ МІЖ СЕРВЕРАМИ ЛОМ

Ю.І. ГОРБЕНКО, О.С. ТОЦЬКИЙ

Обґрунтовуються вимоги, наводяться результати аналізу рівня безпечності стандартизованих криптографічних протоколів автентифікації, пропонується удосконалений криптографічний протокол автентифікації та встановлення ключів між серверами ЛОМ.

The paper proves requirements, presents the results of analyzing the security level of standardized cryptographic authentication protocols, offers an improved cryptographic protocol of authentication and installation of keys between LAN servers.

ВСТУП

В процесі аналізу будемо спиратись на добре розроблено міжнародну систему автентифікації. Вона сьогодні представлена сукупністю випробуваних міжнародних стандартів ISO/IEC 10181-2 [1], національних стандартів ДСТУ ISO/IEC 9797-1 [2], ДСТУ ISO/IEC 9797-2 [3], ДСТУ ISO/IEC 15946-1 [4], ДСТУ ISO/IEC 15946-3 [7], ДСТУ ISO/IEC 9798-3[6]; міжнародних стандартів (проектів національних) ISO/IEC 9798-1, ISO/IEC 9798-2 [8,9], ISO/IEC 9798-4; ISO/IEC 9798-5, ISO/IEC 9798-6 та ISO/IEC 15946 – 2 [5]. В найбільш узагальненому виді автентифікація забезпечує гарантії заявлених ідентифікаційний даних об'єкту. Автентифікація може розглядатися тільки в контексті взаємовідносин між комітентом та об'єктом, що перевіряє – тобто перевірником. Автентифікація, у залежності від особливості її здійснення, може бути зведена до двох варіантів:

– комітента представляє пред'явник, який має особисті комунікаційні взаємовідносини з тим що перевіряє – перевірником (об'єктна автентифікація – entity authentication);

– комітент є ресурсом елементу даних, який доступний перевірнику (оригінальна ідентифікація даних – data origin authentication).

У цілому автентифікація об'єкту забезпечує підтвердження ідентифікаційних даних комітента в рамках комунікаційних взаємовідносин. Автентифіковані дані комітента підтверджуються тільки тоді, коли надається такий сервіс.

Такий тип автентифікації зобов'язує додатково надавати гарантії щодо цілісності та справжності даних, тобто що дані не були підмінені. Це тягне за собою залучення додаткових механізмів автентифікації, перевірки цілісності та справжності.

Як слідує із [1-11], методи та механізми автентифікації є основним надійним засобом криптографічного захисту інформації та ресурсів від НСД. Вони можуть бути реалізованими у вигляді стандартних криптографічних протоколів. Разом з тим, застосування тих чи інших протоколів, необхідно робити у залежності від вимог до захисту від НСД, а також від архітектури та характеристик автоматизованої системи управління (АСУ) та телекомунікаційних мереж (ТМ).

Механізми автентифікації, що рекомендуються діючими міжнародними та національними стандартами [1-21], тісно пов'язані з криптографічними перетвореннями. У цілому механізми автентифікації можна визначити ґрунтуючись на понятті механізму криптографічного перетворення.

Криптографічний механізм автентифікації – це конкретний процес, криптографічний протокол або криптографічний алгоритм, що використовується для реалізації визначених послуг та/або функцій криптографічного захисту інформації та інформаційних ресурсів в частині встановлення достовірності твердження, що [об'єкт] [суб'єкт] має очікувані властивості

В цій статі наводяться результати аналізу та вибору криптографічних механізмів та протоколів взаємної автентифікації об'єктів та встановлення ключів між серверами безпеки різних ЛОМ згідно ДСТУ ISO/IEC 9798–3, ДСТУ ISO/IEC 15946–3 та ДСТУ ISO/IEC 11770–3. При чому для автентифікації серверів різних ЛОМ та установлення ключів конфіденційного обміну, а також їх автентифікації з метою захисту від НСД, пропонується використати у залежності від вимог різні криптографічні протоколи. Розробляється та аналізується удосконалений криптографічний протокол, з тією відмінністю від криптографічного протоколу 5 [11], що маркери передачі ключів сеансу передаються у підписаному вигляді з використанням алгоритму ДСТУ 4145–2002 [19], в тому числі функції гешування ГОСТ 34.311-95. Перевірка цілісності та справжності маркерів здійснюється у відповідності з ДСТУ 4145-2002 та з використанням сертифікатів ключів електронного цифрового підпису. Порівнюються перспективні криптографічні протоколи із ДСТУ ISO/IEC 9798–3, ДСТУ ISO/IEC 15946–3 та ДСТУ ISO/IEC 11770– 3 і як основний результат розробляється удосконалений криптографічний протокол, що забезпечує необхідний рівень захищеності згідно вимог найбільш високого 4 класу захищеності .

В висновках та рекомендаціях наводиться порівняльний аналіз криптографічних механізмів та протоколів автентифікації та встановлення ключів На основі порівняльного аналізу формулюються рекомендації та пропозиції з реалізації

захисту від НСД засобом застосування криптографічних протоколів автентифікації, узгодження та у цілому встановлення ключів.

1 АНАЛІЗ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ НА ОСНОВІ ДСТУ ISO/IEC 9798-3

Механізми взаємної автентифікації забезпечують виконання перевірки автентичності (справжності) сторін, що беруть участь у механізмі. Стандарт ДСТУ ISO/IEC 9798-3 регламентує три механізми взаємної автентифікації. Два з них послідовні – це двох прохідний та трьох прохідний механізми, та паралельний двох прохідний механізм. Послідовні механізми взаємної автентифікації є адаптованими механізмами однобічної автентифікації. В обох випадках це потребує одного додаткового обміну і додатково двох кроків. Удосконалення наведених протоколів забезпечує аналогічну стійкість та рівень безпеки.

В якості базового варіанта взаємної автентифікації між серверами безпеки різних ОА виберемо механізм з двома проходами. Даний механізм автентифікації виконується у два проходи та два кроки і базується на однопрохідному механізмі однобічної автентифікації. На рис. 1 показано даний механізм, при цьому ініціатором може бути як об'єкт *A* так і об'єкт *B*. Як зображено на рис. 1 на першому проході даного механізму об'єкт *A* є пред'явником для об'єкта *B*, який представляє перевірника. На другому проході об'єкт *B* є пред'явником для об'єкта *A*, який представляє перевірника.

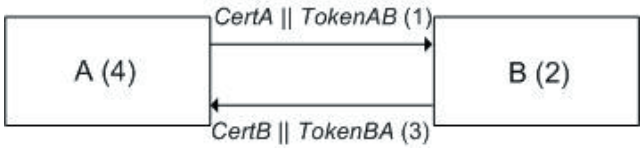

Рис. 1. Взаємна автентифікація з двома проходами

Форма маркера (*TokenAB*), що відсилається об'єктом *A* об'єкту *B* ідентична формі маркеру визначеного в однопрохідному механізмі однобічної автентифікації.

$$TokenAB = \begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text2 \| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1 \right). \quad (1)$$

Форма маркера (*TokenBA*), що відсилається об'єктом *B* об'єкту *A*:

$$TokenBA = \begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text4 \| sS_B \left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text3 \right). \quad (2)$$

Для формування маркерів *TokenAB* та *TokenBA* об'єкти *A* та *B* використовують або порядкові номера N_A, N_B відповідно, або позначки часу T_A, T_B відповідно, у якості змінних у часі параметрів формують підписи $sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1 \right)$, $sS_B\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text3 \right)$ відповідно. *Text*1 та *Text*3 записані дані об'єктів *A* та *B* відповідно. Вибір у використанні в якості змінних у часі параметрів порядкових номерів або позначок часу залежить від технічних можливостей пред'явника та перевірника, а також від оточення.

Механізм, що наведено на рис. 1 описується таким чином.

1) Об'єкт *A* відсилає об'єкту *B* маркер *TokenAB*, а також (не обов'язково) свій сертифікат.

2) Після отримання повідомлення, що містить *TokenAB*, об'єкт *B* виконує такі кроки:

одержує від уповноваженого на розподілення сертифікатів сертифікат пред'явника *A*, або використовує сертифікат, який надіслано пред'явником. Перевіряє, що має дійсний відкритий ключ пред'явника. Одержує від ТДС перевірочну ІА для заявленої ІА пред'явника;

перевіряє коректність маркера *TokenAB* шляхом:

– перевірки цифрового підпису, що міститься у маркері, використовуючи перевірочну ІА об'єкта *A*, позначку часу T_A або порядковий номер N_A, розпізнавальний ідентифікатор B;

– перевірки коректності позначки часу або порядкового номера;

– порівняння ідентичності значення поля ідентифікатора *B* в підписаних даних маркера *TokenAB* та розпізнавального ідентифікатора об'єкта *B*.

3) Об'єкт *B* генерує та відсилає маркер *TokenBA* об'єкту *A*, а також (не обов'язково) свій сертифікат.

4) Повідомлення крок (3) обробляється аналогічно до кроку (2)

Після отримання повідомлення, що містить *TokenBA*, об'єкт *A* виконує такі кроки:

одержує від уповноваженого на розподілення сертифікатів сертифікат пред'явника *B*, або використовує сертифікат, який надіслано пред'явником. Перевіряє, що має дійсний відкритий ключ пред'явника, одержує від ТДС перевірочну ІА для заявленої ІА пред'явника;

перевіряє коректність маркера *TokenBA* шляхом:

– перевірки цифрового підпису, що міститься у маркері, використовуючи перевірочну ІА, позначку часу T_B або порядковий номер N_B та розпізнавальний ідентифікатор *A*;

– перевірки коректності позначки часу або порядкового номера;

– порівняння ідентичності значення поля ідентифікатора *A* в підписаних даних маркера *TokenBA* та розпізнавального ідентифікатора об'єкта *A*.

Два повідомлення даного механізму пов'язані між собою лише вимогою відносної своєчасності, для подальшого зв'язування цих повідомлень можна використовувати додатково відповідні текстові поля.

Аналіз стійкості кожного проходу даного механізму до атак типу «Підміна» та «Повтор»

наведено в [1,10] при розгляді однопрохідного механізму однобічної автентифікації. Проведемо аналіз відносно можливості протистояння даним атакам для цілісного механізму. Для встановлення взаємної автентифікації даний механізм використовує два проходи для передавання обмінної ІА, яка містить унікальні числа, які представлено позначками часу T_A та T_B, або порядкові номери N_A та N_B відповідно, унікальні характеристики обраних перевірників, які представлено розпізнавальним ідентифікатором B для першого проходу, та розпізнавальним ідентифікатором A для другого проходу, заявленою ІА об'єкта A, яка представлена тестовим полем $Text1$, та заявленою ІА об'єкта B, яка представлена текстовим полем $Text3$. Заявлена ІА схована від зловмисника. У цілому за класифікацією вразливостей механізмів автентифікації, які представлено у стандарті ISO/IEC 10181-2, даний механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4а «Механізми з унікальним числом».

Для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу.

Для реалізації атаки типу «Підміна» зловмиснику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричних цифрових підписів, що рекомендується використовувати з даним механізмом автентифікації, то складність підробки цифрового підпису повинна бути не меншою ніж експонентною.

Даний механізм можна використовувати разом з протоколами встановлення та розподілення ключів, що наведено у стандарті ISO/IEC 11770-2,3, для управління ключовою інформацією. Наприклад, для встановлення конфіденційного ключа з підтвердженням та взаємної автентифікації, де ініціатором є пред'явник, можна даний механізм представити таким чином.

Об'єкт B одержує маркер $TokenAB$, перевіряє його та формує за допомогою криптографічної контрольної функції v та ключа K_{AB} конфіденційний ключ

$$K = v_{K_{AB}}\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| sS_A\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Text1\right)\right), \qquad (4)$$

та зашифровує на цьому ключі маркер $TokenBA$

$$TokenBA = e_K\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text4 \| sS_B\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Text3\right)\right); \qquad (5)$$

Об'єкт A одержує з маркеру, що сформовано на першому проході, необхідні дані, виробляє ключ K та розшифровує одержаний маркер $TokenBA$. А далі робить всі перевірки згідно даного механізму, як описано вище.

Таким чином модифікований механізм може забезпечувати взаємну автентифікацію та встановлення конфіденційного ключа з підтвердженням.

Необхідність існування третьої довіреної сторони продиктована необхідністю одержання перевірником B перевірочної ІА для перевірки цифрового підпису sS_A, а також одержання та перевірки статусу сертифікату пред'явника A для першого проходу. І навпаки для об'єктів B у якості пред'явника та A у якості перевірника на другому проході. Управління сертифікатами відкритих ключів покладається на уповноваженого на сертифікацію, наприклад PKI [24]. Розподіл перевірочної ІА покладається на уповноваженого домену безпеки, в якому знаходиться пред'явник. При цьому уповноважений домену безпеки може використовуватися у інтерактивній або автономній автентифікації. У інтерактивному режимі автентифікації уповноважений домену використовується пред'явником для генерування обмінної ІА, а перевірником для підтримки його у перевірці обмінної ІА. У автономному режимі уповноважений домену безпеки у автономному режимі завчасно генерує та розподіляє сертифікати автономної автентифікації, які пізніше використовуються перевірником для підтвердження обміну при автентифікації.

Основним недоліком криптографічного протоколу, що наведений вище в пункті 1, є необхідність розповсюдження та у цілому управління ключами симетричної криптографічної функції на рівні корпоративної автоматизованої системи 3 рівня (АС – 3) для обчислень криптографічного значення згідно виразу 4.

2. АНАЛІЗ ТА ВИБІР КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ ВЗАЄМНОЇ АВТЕНТИФІКАЦІЇ ОБ'ЄКТІВ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ МІЖ СЕРВЕРАМИ БЕЗПЕКИ ДСТУ ISO/IEC 11770 – 3[11]

Для автентифікації серверів різних ЛОМ та установлення ключів конфіденційного обміну, а також їх автентифікації з метою захисту від НСД, розглянемо криптографічний протокол 5 (5) згідно ДСТУ ISO/IEC 11770–3.

Сутність та аналіз протоколу 5(5) [11] узгодження ключів та автентифікації.

Протокол 5 забезпечує встановлення таємного ключа (таємниці) що розділюється між суб'єктами A і B за два проходи. Протокол забезпечує взаємну неявну автентифікацію цього таємного ключа і сумісне управління ключами. Повинні виконуватись такі вимоги:

а) кожен суб'єкт X має особистий ключ $h_X \in H$ для узгодження ключів і відкритий ключ $p_X = F(h_X, g)$ для узгодження ключів;

б) кожен суб'єкт має доступ до автентифікованої копії відкритого ключа для узгодження ключів іншого суб'єкта;

в) обидва суб'єкта повинні узгодити та використовувати однакову одно направлену функцію w.

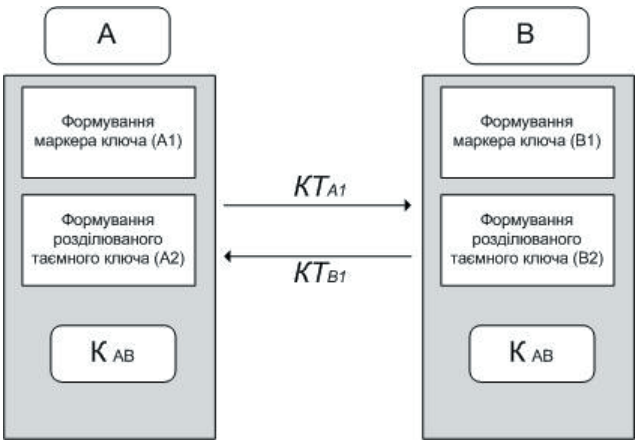

Рис. 3. Узгодження ключів, протокол 5

Формування маркера ключа ($A1$). Суб'єкт A генерує випадкове таємне число $r_A \in H$, обчислює $F(r_A, g)$, формує маркер ключа:

$$KT_{A1} = F(r_A, g) \| Text1 \quad (6)$$

і надсилає його суб'єкту B.

Формування маркера ключа ($B1$). Суб'єкт B генерує випадкове таємне число $r_B \in H$, обчислює $F(r_B, g)$, формує маркер ключа:

$$KT_{B1} = F(r_B, g) \| Text2 \quad (7)$$

і надсилає його суб'єкту A.

Формування розділюваного таємного ключа ($B2$). Суб'єкт B виділяє $F(r_A, g)$ з одержаного маркера ключа KT_{A1} і обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(h_B, F(r_A,g)),F(r_B,p_A)), \quad (8)$$

де w є однонаправленою функцією.

Формування розділюваного таємного ключа ($A2$). Суб'єкт A виділяє $F(r_B, g)$ з одержаного маркера ключа KT_{B1} і обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(r_A, p_B), F(h_A, F(r_B, g))), \quad (9)$$

Наведений протокол 5 має такі властивості.

1. При кожному узгодженні розділюваного таємного ключа встановлюється новий розділюваний таємний ключ і на основі нього новий таємний ключ. Це досягається за рахунок використання сеансових ключів особистих r_A та r_B, а також відкритих $F(r_A, g)$, $F(r_B, g)$.

2. При узгодженні розділюваного таємного ключа обидва суб'єкти в однаковій мірі впливають на обчислення розділюваного таємного ключа, він є залежним як від сеансових так і статичних (довгострокових) ключів.

3. Попередньо суб'єкти A та B повинні одержати доступ до сертифікатів відкритих ключів один одного, відповідно P_A та P_B.

4. Попередньо обчислення здійснити не можна, так як при кожному обчисленні використовуються сеансові ключі.

5. Протокол ґрунтується на використанні відкритих статичних асиметричних пар ключів, цю функцію може виконувати третя довірча сторона, виготовляючи та забезпечуючи життєвий цикл сертифікатів відкритих ключів відповідно P_A та P_B.

З урахуванням рекомендацій міжнародного стандарту ISO/IEC 9594-8‖X-509 ITU, а також закону України «Про електронний цифровий підпис» в якості відкритих ключів P_A та P_B необхідно використовувати сертифікати вказаних відкритих ключів.

7. При використанні протоколу неспростовність суб'єктів A та B забезпечується за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B та відповідних сертифікатів P_A та P_B.

8. В протоколі 5 забезпечується взаємна криптоживучість розділюваного таємного ключа, що досягається використанням на кожному сеансі пари сеансових ключів r_A та r_B. При цьому, компрометація сеансового чи довгострокового ключа (окремо) не приводить до компрометації розділюваного таємного ключа.

9. При записі в полі $Text2$ криптографічного контрольного значення на відомих даних, що обчислюється з використанням ключа K_{AB}, протокол забезпечує підтвердження розділюваного таємного ключа суб'єкту A суб'єктом B, а значить з урахуванням неявної автентифікації явну автентифікацію розділюваного таємного ключа суб'єктом B суб'єкта A.

10. Забезпечується взаємна неявна автентифікація розділюваного таємного ключа між суб'єктами A та B, а також явна автентифікація розділюваного таємного ключа суб'єктом B суб'єкта A.

11. При використанні протоколу неспростовність суб'єктів A та B забезпечується в неявному вигляді за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B та відповідних сертифікатів p_A та p_B.

12. Проведений аналіз показав, що для обчислення розділюваного таємного ключа порушник повинен, як мінімум, розв'язати наступні задачі (наприклад, через атаку на абонента A):

– одержати сертифікат ключа p_A та розв'язати задачу обчислення відповідного йому особистого ключа h_A;

– перехопити маркер ключа KT_{B1} ;

перехопити маркер ключа KT_{A1} та розв'язати задачу обчислення особистого ключа сеансу r_A;

– одержати сертифікат відкритого ключа p_B.

Знаючи односторонню функцію ω обчислити розділюваний таємний ключ K_{AB}.

Таким чином, при здійсненні атаки типу повне розкриття порушник повинен як мінімум розв'язати дві задачі визначення особистих – статичного (довгострокового) та сеансового ключів, для суб'єкта A – h_A та r_A, для суб'єкта B – h_B та r_B. Ці задачі носять експонентний характер складності (в групі точок еліптичних кривих). При виборі відповідних розмірів параметрів (а вони в стандарті зафіксовані) вказані задачі на сучас-

ному етапі розвитку практично не можуть бути розв'язаними.

Слід зауважити, що при успішній атаці типу «повне розкриття» , компрометованим буде тільки один розділюваний таємний ключ.

У цілому протокол 5 узгодження ключів є одним із найбільш захищеним, при його використанні забезпечується крипто живучість розділюваного конфіденційного ключа, автентифікація ключів та підтвердження розділюваного таємного ключа, що виробляється. Протокол практично є захищеним від атаки типу «повне розкриття», так як для її здійснення необхідно розв'язати дві експонентні складні задачі (за умови використання криптографічного перетворення в групі точок еліптичних кривих).

Для захисту маркерів від атак типу «повтор» можна використовувати поля маркерів *Text* 1 та *Text* 2.

В той же час, при його здійсненні суб'єкти повинні виконувати в плинному часі складні обчислення. Головним же недоліком наведеного протоколу є те що на першому етапі маркери передаються у не захищеному вигляді, без контролю їх цілісності та автентичності, а також без авторизації джерел формування цих маркерів.

Нижче наводиться комбінований протокол автентифікації, встановлення та підтвердження ключів, що побудований на послідовному використанні двох протоколів – протоколу цифрового підпису маркерів та протоколу 5, що наведений вище.

3. УДОСКОНАЛЕНИЙ КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ВЗАЄМНОЇ АВТЕНТИФІКАЦІЇ ОБ'ЄКТІВ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ МІЖ СЕРВЕРАМИ БЕЗПЕКИ

Нижче наводиться комбінований протокол автентифікації та встановлення ключів (спільної таємниці), що побудований на послідовному використанні двох протоколів – протоколу цифрового підпису маркерів та протоколу 5, що наведений вище.

Удосконалений протокол забезпечує взаємну автентифікацію та встановлення розділюваного таємного ключа між суб'єктами A і B за два проходи. Протокол забезпечує також сумісне управління ключами, встановлення та підтвердження таємниці та ключів, що обумовлено використанням асиметричного цифрового підпису згідно ДСТУ 4145 – 20002 та шифрування.

Повинні виконуватись такі вимоги:

а) суб'єкт A має асиметричну систему підпису з перетворенням (S_A, V_A);

б) суб'єкт B має асиметричну систему підпису з перетворенням (S_B, V_B);

в) кожен суб'єкт X має особистий ключ $h_X \in H$ для встановлення ключів і відкритий ключ $p_X = F(h_X, g)$ для встановлення ключів;

г) кожен суб'єкт має доступ до автентифікованої копії відкритого ключа для встановлення ключів іншого суб'єкта.

д) обидва суб'єкти повинні узгодити та використовувати однакові загально – системні параметри криптографічних перетворень;

є) обидва суб'єкти повинні узгодити та використовувати однакову одно направлену функцію w.

Формування маркера ключа ($A1$). Суб'єкт A генерує випадкове таємне число $r_A \in H$, обчислює $F(r_A, g)$, формує маркер ключа та підписує його використовуючи особистий ключ (перетворення) S_A:

$$KT_{A1} = S_A(F(r_A, g) \parallel Text1) \qquad (10)$$

і надсилає його суб'єкту B.

В полі *Text*1 обов'язковими складовими є розрізнювальні ідентифікатори пред'явника та перевірника, а також номери (випадкові числа) або часові мітки захисту від атак типу «повтор».

У випадку використання для здійснення ЕЦП перетворень в групі точок еліптичних кривих [4, 19] над відповідним полем Галуа, функція $F(r_A,g)$ має вигляд

$$F(r_A, g) = r_A\, G(\mathrm{mod}\ q),$$

де G – порядок базової точки, q – модуль перетворення.

Формування маркера ключа ($B1$). Суб'єкт B генерує випадкове таємне число $r_B \in H$, обчислює $F(r_B, g)$, формує маркер ключа та підписує його використовуючи особистий ключ (перетворення) S_B:

$$KT_{B1} = S_B(F(r_B, g) \parallel Text2) \qquad (11)$$

і надсилає його суб'єкту A.

У полі *Text*2 обов'язковими складовими є розрізнювальні ідентифікатори пред'явника та перевірника, а також номери (випадкові числа) або часові мітки захисту від атак типу «повтор».

У випадку використання для здійснення ЕЦП перетворень в групі точок еліптичних кривих [4, 19] над відповідним полем Галуа, функція $F(r_B,g)$ має вигляд

$$F(r_B, g) = r_B\, G(\mathrm{mod}\ q), \qquad (12)$$

де G – порядок базової точки, q – модуль перетворення.

Формування розділюваного таємного ключа ($B2$). Суб'єкт B перевіряє цілісність та справжність (автентичність) маркера KT_A використовуючи сертифікат відкритого ключа електронного цифрового підпису (перетворення) V_A, потім виділяє $F(r_A, g)$ з одержаного маркера ключа KT_{A1} і обчислює розділюваний таємний ключ (розділювану таємницю):

$$K_{AB} = w(F(h_B, F(r_A,g)), F(r_B,p_A)), \qquad (13)$$

де w є одно направленою функцією. З урахуванням вимог національного законодавства в якості одно направленої функції можна вибрати міждержавний стандарт ГОСТ 34.311 – 95 або дозволений Державною службою інший стандарт гешування,

наприклад згідно проекту ДСТУ ISO/IEC 9797 – 2 [2] або при наявності дозволу ISO/IEC 10118 чи ISO/ IEC 15946-2.

У випадку використання при обчисленні розділюваної таємниці перетворень в групі точок еліптичних кривих [7] над відповідним полем Галуа, функція $F(h_B, F(r_A,g))$ має вигляд

$$F(h_B,F(r_A,g)) = h_B\, F(r_A,g)(\mathrm{mod}\ q), \qquad (14)$$

де $F(r_A,g)$ – точка еліптичної кривої, що обчислена вище.

Функція $F(r_B, p_A)$ обчислюється у вигляді скалярного добутку та має вигляд

$$F(r_B, p_A) = r_B\, p_A(\mathrm{mod}\ q), \qquad (15)$$

де p_A – сертифікат відкритого ключа абонента A.

Формування розділюваного таємного ключа ($A2$). Суб'єкт A перевіряє цілісність та справжність (автентичність) маркера KT_{B1} використовуючи сертифікат відкритого ключа електронного цифрового підпису (перетворення) V_B, виділяє $F(r_B,g)$ з одержаного маркера ключа KT_{B1} і обчислює розділюваний таємний ключ:

$$K_{AB} = w(F(r_A,p_B), F(h_A, F(r_B,g))), \qquad (16)$$

де w є одно направленою функцією.

Аналогічно, як вказувалось вище, в якості одно направленої функції можна вибрати міждержавний стандарт гешування ГОСТ 34.311 – 95 [21] або дозволений Державною службою інший стандарт гешування, наприклад згідно проекту ДСТУ ISO/IEC 9797 – 2[3].

У випадку використання при обчисленні розділюваної таємниці перетворень в групі точок еліптичних кривих [7,11] над відповідним полем Галуа, функція $F(h_A, F(r_B, g))$ має вигляд

$$F(h_A, F(r_B, g)) = h_A\, F(r_B, g)(\mathrm{mod}\ q), \qquad (17)$$

де $F(r_B, g)$ – точка еліптичної кривої, що обчислена вище.

Функція $F(r_A, p_B)$, обчислюється у вигляді скалярногоо добутку та має вигляд

$$F(r_A, p_B) = r_A\, p_B(\mathrm{mod}\ q), \qquad (18)$$

де p_B – сертифікат відкритого ключа абонента B.

Необхідно відмітити, що абоненти A та B при обчисленні розділюємої таємниці K_{AB} повинні узгодити правило об'єднання координат точок еліптичної кривої. Згідно [2, 14] для об'єднання можна використовувати операцію конкатенації координат двох точок в узгодженій послідовності.

ВИСНОВКИ

Удосконалений протокол автентифікації та встановлення ключів (в подальшому протокол автентифікації та встановлення ключів між серверами безпеки різних ЛОМ) має суттєві переваги перед іншими, в тому числі:

– завжди забезпечується явна взаємна автентифікація абонентів, що ґрунтується на використанні особистих ключів цифрового підпису та сертифікатів відповідних відкритих ключів іншого абонента при пересиланні підписаних маркерів $KTA1$ та KTB1;

– забезпечується цілісність та справжність маркерів $KTA1$ та $KTB1$ при їх передаванні та на усіх етапах життєвого циклу, тобто виключається можливість здійснення активних атак на удосконалений криптографічний протокол (за виключенням атаки типу «повне розкриття», складність якої носить експонентний характер);

– при кожному узгодженні розділюваного таємного ключа встановлюється новий розділюваний таємний ключ, що досягається за рахунок використання ключів сеансу (особистих) rA та rB, а також відкритих $F(rA, g)$, $F(rB, g)$, які передаються між абонентами з забезпеченням їх цілісності та справжності;

– при узгодженні розділюваного таємного ключа обидва суб'єкти в однаковій мірі впливають на обчислення розділюваного таємного ключа, він є залежним як від сеансових так і статичних (довгострокових) ключів;

– суб'єкти A та B попередньо повинні одержати доступ до сертифікатів відкритих ключів один одного, відповідно до P_A та P_B встановлення ключів, а також V_A та V_B перевірки електронних цифрових підписів;

– удосконалений протокол ґрунтується на використанні відкритих статичних асиметричних пар P_A та P_B встановлення ключів та електронних цифрових підписів V_A та V_B, цю функцію може виконувати третя довірча сторона, виготовляючи та забезпечуючи життєвий цикл сертифікатів відкритих ключів відповідно P_A та P_B, а також V_A та V_B;

– з урахуванням рекомендацій міжнародного стандарту ISO/IEC 9594-8‖X-509 ITU, а також закону України "Про електронний цифровий підпис" в якості відкритих ключів P_A та P_B необхідно використовувати сертифікати відповідно P_A та P_B, а також в якості відкритих ключів електронного цифрового підпису сертифікати V_A та V_B;

– при використанні протоколу неспростовність суб'єктів A та B забезпечується за рахунок використання кожним із суб'єктів особистих ключів h_A та h_B та відповідних сертифікатів P_A та P_B встановлення ключів, а також особистих ключів S_A та S_B електронного цифрового підпису та сертифікатів відкритих ключів електронного цифрового підпису V_A та V_B;

– в протоколі забезпечується взаємна крипто живучість розділюваного таємного ключа, що досягається використанням на кожному сеансі пари сеансових ключів r_A та r_B, причому, компрометація сеансового чи довгострокового ключа (окремо) не приводить до компрометації розділюваного таємного ключа;

– при записі в полі $Text2$ криптографічного контрольного значення на відомих даних, що обчислюється з використанням ключа K_{AB}, про-

токол забезпечує підтвердження розділюваного таємного ключа суб'єкту *A* суб'єктом *B*;

– забезпечується взаємна неявна автентифікація розділюваного таємного ключа між суб'єктами *A* та *B*, а також явна автентифікація розділюваного таємного ключа суб'єктом *B* суб'єкта ;.

– для встановлення взаємної автентифікації даний механізм використовує два проходи для передавання обмінної ІА, яка містить унікальні числа, які представлено позначками часу T_A та T_B, або порядкові номери N_A та N_B відповідно, яка представлена в тестових полях *Text*1 та *Text*2 . Заявлена ІА захищена від порушника (зловмисника). У цілому за класифікацією вразливостей механізмів автентифікації, які представлено у стандарті ISO/IEC 10181-2, даний механізм підпадає під клас 4 «Механізми, що захищені від розкриття заявленої ІА та атак типу «Повтор» на одного та різних перевірників», проміжний клас 4а «Механізми з унікальним числом» та цифровим підписом;

– для протистояння атаці типу «Повтор» також використовується цифровий підпис для надання послуги цілісності від даних автентифікації та позначок часу або порядкових номерів. Для синхронізації часу необхідно використовувати систему загальної координації часу;

– для реалізації атаки типу «Підміна» зловмиснику необхідно підробити підпис від нового значення унікального числа та заявленої ІА. Згідно з потребами стійкості до підробок асиметричного цифрового підпису, що рекомендується використовувати з даним механізмом автентифікації, то складність підробки цифрового підпису повинна бути не меншою ніж експонентна;

– у якості цифрового підпису пропонується використовувати алгоритм цифрового підпису ДСТУ 4145: 2002, який схвалений для застосування з метою захисту інформації, що є власністю Держави, спеціальним уповноваженим органом державного управління в сфері криптографічного захисту інформації;

– у стандарті ДСТУ 4145 пропонується використовувати генератор випадкових послідовностей визначений цим стандартом, або інший генератор випадкових послідовностей, рекомендований уповноваженим органом державної влади у сфері криптографічного захисту інформації для отримання випадкових цілих чисел, випадкових елементів основного поля та випадкових точок еліптичних кривих.

У цілому розроблений на основі комбінування протоколу електронного цифрового підпису та протоколу 5 встановлення ключів удосконалений протокол автентифікації та встановлення ключів є найбільш захищеним. При його використанні забезпечується явна автентифікація абонентів, неявна автентифікація ключів, крипто живучість розділюваного таємного ключа та, при необхідності, підтвердження розділюваного таємного ключа, що виробляється. Протокол практично є захищеним від атаки типу повне розкриття, так як для її здійснення необхідно розв'язати дві експонентні складні задачі.

Література.

[1] ISO/IEC 10181-2:1996 Information technology – Open Systems Interconnection -– Security frameworks for open systems: Authentication framework

[2] ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[3] ISO/IEC 9797-2, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.

[4] ISO/IEC 15946-1:20011, Інформаційні технології – Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих – Частина 1: Загальні положення

[5] ISO/IEC 15946-2:20011, Інформаційні технології – Методи захисту – Криптографічні перетворення, що ґрунтуються на еліптичних кривих – Частина 2: Цифрові підписи.

[6] ДСТУ ISO/IEC 9798 – 3: 2002. Інформаційні технології. Методи захисту. Автентифікація обєктів. Частина 3: Механізми, що грунтуються на цифровому підписі (ISO/IEC 9798 – 3: 2002, IDT)

[7] ДСТУ ISO/IEC 15946 – 3:2006. Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Встановлення ключів (ISO/IEC 15946 – 3:2002, IDT).

[8] ISO/IEC 9798-1 Information technology – Security techniques – Entity authentication – Part1: General.

[9] ISO/IEC 9798-2 Information technology – Security techniques – Entity authentication – Part2: Mechanisms using symmetric encipherment algorithms.

[10] ISO/IEC 9798-3 Information technology – Security techniques – Entity authentication – Part3: Mechanisms using digital signature techniques

11] ДСТУ ISO/IEC 11770-3-2002 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів (ISO/IEC 11770-3:1999, IDT).

[12] ДСТУ ISO/IEC 14888-1-2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC 14888-1:1998:, IDT).

[13. ДСТУ ISO/IEC 14888-2-2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів (ISO/IEC 14888-2:1999, IDT).

[14] ДСТУ ISO/IEC 14888-3-2002 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів (ISO/IEC 14888-3:1998, IDT).

[15] AC/35 – N/271 – «General Guidance on the Security jf Automatic Data Processing Systems and networks».

[16] За загальною редакцією академіка НАН України В.П. Горбуліна. Основи інформаційної безпеки та захисту інформації у контексті Євроатлантичної інтеграції України. ДП «НВЦ» Євроатлантикінформ». Київ, 2006,103с.

[17] *Боков А, Ю., Рахманов О.В.* Обзор технологии пластиковых карт //Безопасность информационных технологий.– 1999.– №2.

[18] *Л.К.Бабенко, С.С. Ищуков, О.Б. Макаревич*. Защита информации с использованием смарт – карт и электронных брелоков. Москва, Гелиос – АРВ, 2003, 351 с.

[19] ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка.

[20] ДСТУ ISO/IEC 15946–1:2006. Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946 – 1:2002, IDT).

[21] ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция гешированя.

[22] *І.Д. Горбенко, Т.О. Гриненко.* Захист інформації в інформаційно-телекомунікаційних системах. Частина 1. Криптографічний захист інформації. Навчальний посібник. МОНУ. Харків. 2004. 368 с.

[23] *Б. Шнайер.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты та языке Си. – Москва. «Триумф». 2002. – 797 с.

[24] Закон України Про електронний цифровий підпис. (Відомості Верховної Ради (ВВР), 2003, N 36, ст.276).

Надійшла до редколегії 25.09.2009

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор ЗАТ «ІІТ», науковий співробітник НІЦ «Z» каф. БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах.

Тоцький Олександр Сергійович, спеціаліст кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах.